

# Criteria for Finite Difference Gröbner Bases of Normal Binomial Difference Ideals\*

Yu-Ao Chen and Xiao-Shan Gao

KLMM, UCAS, Academy of Mathematics and Systems Science  
The Chinese Academy of Sciences, Beijing 100190, China

## Abstract

In this paper, we give decision criteria for normal binomial difference polynomial ideals in the univariate difference polynomial ring  $\mathcal{F}\{y\}$  to have finite difference Gröbner bases and an algorithm to compute the finite difference Gröbner bases if these criteria are satisfied. The novelty of these criteria lies in the fact that complicated properties about difference polynomial ideals are reduced to elementary properties of univariate polynomials in  $\mathbb{Z}[x]$ .

**Keywords.** Difference algebra, binomial difference ideal, Gröbner basis, difference Gröbner basis.

## 1 Introduction

Difference algebra founded by Ritt and Cohn aims to study algebraic difference equations in a similar way that polynomial equations are studied in commutative algebra and algebraic geometry [5, 14, 18, 21]. The Gröbner basis invented by Buchberger is a powerful tool for solving many mathematical problems [4]. The concepts of difference Gröbner bases was extended to linear difference polynomial ideals in [11, 14, 15] and nonlinear difference polynomial ideals in [11]. Many applications of difference Gröbner bases were given [9, 14–16].

Since difference polynomial ideals can be infinitely generated, their difference Gröbner bases are generally infinite. Even for finitely generated difference polynomial ideals, their difference Gröbner bases could be infinite as shown by Example 2.2 in this paper. This makes it impossible to compute difference Gröbner bases for general difference polynomial ideals and thus it is a crucial issue to give criteria for difference polynomial ideals to have finite difference Gröbner bases.

Let  $\mathcal{F}$  be a difference field and  $y$  a difference indeterminate. In this paper, we will give decision criteria for normal binomial difference polynomial ideals in  $\mathcal{F}\{y\}$  to have finite difference Gröbner bases and an algorithm to compute these finite difference Gröbner bases under these criteria. A difference ideal  $\mathcal{I}$  in  $\mathcal{F}\{y\}$  is called normal if  $MP \in \mathcal{I}$  implies  $P \in \mathcal{I}$  for any difference monomial  $M$  in  $\mathcal{F}\{y\}$  and  $P \in \mathcal{F}\{y\}$ .  $\mathcal{I}$  is called binomial if it is generated by difference polynomials with at most two terms [6, 7].

For  $f \in \mathbb{Z}[x]$ , let  $f^+, f^- \in \mathbb{N}[x]$  be the positive part and the negative part of  $f$  such that  $f = f^+ - f^-$ . For  $h = \sum_{i=0}^m a_i x^i \in \mathbb{N}[x]$ , denote  $y^h = \prod_{i=0}^m (\sigma^i y)^{a_i}$ , where  $\sigma$  is the difference operator of  $\mathcal{F}$ . Then any difference monomial in  $\mathcal{F}\{y\}$  can be written as  $y^g$  for some  $g \in \mathbb{N}[x]$ . For a given  $f \in \mathbb{Z}[x]$  with a positive leading coefficient, we consider the following binomial difference polynomial ideal in  $\mathcal{F}\{y\}$ :

$$\mathcal{I}_f = \text{sat}(y^{f^+} - y^{f^-}) = [\{y^{h^+} - y^{h^-} \mid h = gf, g \in \mathbb{Z}[x]\}]$$

---

\*Partially supported by a grant from NSFC 11101411.

where  $\text{sat}$  is the difference saturation ideal to be defined in Section 2 of this paper. Let

$$\begin{aligned}\Phi_0 &\triangleq \{h \in \mathbb{Z}[x] \mid \text{lt}(h) = h^+\}, \\ \Phi_1 &\triangleq \{h \in \mathbb{Z}[x] \mid hg \in \Phi_0 \text{ for some monic polynomial } g \in \mathbb{Z}[x]\}.\end{aligned}$$

We prove that  $\mathcal{I}_f$  has a finite difference Gröbner basis if and only if  $f \in \Phi_1$ . This criterion is then extended to general normal binomial difference ideals in  $\mathcal{F}\{y\}$ .

The decision of  $f \in \Phi_1$  is quite nontrivial and we give the following criteria for  $f \in \Phi_1$  based on the roots of  $f$ :

1. if  $f$  has no positive roots, then  $f \in \Phi_1$ ;
2. if  $f$  has more than one positive roots (with multiplicity counted), then  $f \notin \Phi_1$ ;
3. if  $f$  has one positive root  $x_+$  and a root  $z$  such that  $|z| > x_+$ , then  $f \notin \Phi_1$ ;
4. if  $f$  has one positive root  $x_+$  and a root  $z$  such that  $|z| = x_+$ , then we can compute another  $f^* \in \mathbb{Z}[x]$  and  $x^* \in \mathbb{R}_{>0}$  such that  $f^*(x^*) = 0$ ,  $f^*(w) = 0$  and  $|w| = x^*$  imply  $w = x^*$ , and  $f^*(w) = 0$  and  $|w| \neq x^*$  imply  $|w| < x^*$ . Furthermore,  $f \in \Phi_1$  if and only if  $f^* \in \Phi_1$ ;
5. if  $f \notin \Phi_0$  has a unique positive real root  $x_+$  and  $x_+ < 1$ , then  $f \notin \Phi_1$ ;
6. if  $f(1) = 0$  and any other root  $z$  of  $f$  satisfies  $|z| < 1$ , then  $f \in \Phi_1$  if and only if  $f(x)/(x-1) \in \mathbb{Z}[x^\delta]$  for some  $\delta \in \mathbb{N}_{>0}$  and  $f(x)(x^\delta - 1)/(x-1) \in \Phi_0$ .

With these criteria, only one case is open:  $f$  has a unique positive real root  $x_+$ ,  $x_+ > 1$ , and  $x_+ > |z|$  for any other root  $z$  of  $f$ . We conjecture that  $f \in \Phi_1$  in the above case based on numerical computations. If  $\mathcal{I}_f$  has a finite difference Gröbner basis according to one of the six criteria listed above, we also give an algorithm to compute it.

As far as we know the above criteria are the first non-trivial ones for a difference polynomial ideal to have a finite difference Gröbner basis. The novelty of these criteria lies in the fact that complicated properties about difference polynomial ideals are reduced to elementary properties of univariate polynomials in  $\mathbb{Z}[x]$ .

The rest of this paper is organized as follows. In Section 2, preliminaries on Gröbner basis for difference polynomial ideals are given. In Section 3, criteria for normal binomial difference ideals in  $\mathcal{F}\{y\}$  to have finite difference Gröbner bases are given. In Section 4, criteria for  $f \in \Phi_1$  and an algorithm to compute the finite difference Gröbner basis of  $\mathcal{I}_f$  under these criteria are given. In Section 5, we propose an approach based on integer programming to find  $g$  such that  $fg \in \Phi_0$  and give a lower bound for  $\deg(g)$  in certain cases.

## 2 Preliminaries on Gröbner basis of difference polynomial ideals

### 2.1 Gröbner basis of a difference polynomial ideal

An ordinary difference field, or simply a  $\sigma$ -field, is a field  $\mathcal{F}$  with a third unitary operation  $\sigma$  satisfying: for any  $a, b \in \mathcal{F}$ ,  $\sigma(a+b) = \sigma(a) + \sigma(b)$ ,  $\sigma(ab) = \sigma(a)\sigma(b)$ , and  $\sigma(a) = 0$  if and only if  $a = 0$ . We call  $\sigma$  the *difference or transforming operator* of  $\mathcal{F}$ . A typical example of  $\sigma$ -field is  $\mathbb{Q}(\lambda)$  with  $\sigma(f(\lambda)) = f(\lambda + 1)$ . In this paper, we use  $\sigma$ - as the abbreviation for difference or transformally.

For  $a$  in any  $\sigma$ -extension ring of  $\mathcal{F}$  and  $n \in \mathbb{N}_{>0}$ ,  $\sigma^n(a)$  is called the  $n$ -th transform of  $a$  and denoted by  $a^{x^n}$ , with the usual assumption  $a^0 = 1$  and  $x^0 = 1$ . More generally, for  $p = \sum_{i=0}^s c_i x^i \in \mathbb{N}[x]$ , denote  $a^p = \prod_{i=0}^s (\sigma^i a)^{c_i}$ . For instance,  $a^{3x^2+x+4} = (\sigma^2(a))^3 \sigma(a) a^4$ . It is easy to check that  $a^p$  satisfies the properties of powers [7].

Let  $S$  be a subset of a  $\sigma$ -field  $\mathcal{G}$  which contains  $\mathcal{F}$ . We will denote  $\Theta(S) = \{\sigma^k a \mid k \in \mathbb{N}, a \in S\}$ ,  $\mathcal{F}\{S\} = \mathcal{F}[\Theta(S)]$ . Now suppose  $\mathbb{Y} = \{y_1, \dots, y_n\}$  is a set of  $\sigma$ -indeterminates over  $\mathcal{F}$ . The elements of  $\mathcal{F}\{\mathbb{Y}\}$  are called  $\sigma$ -polynomials over  $\mathcal{F}$  in  $\mathbb{Y}$ . A  $\sigma$ -polynomial ideal  $\mathcal{I}$ , or simply a  $\sigma$ -ideal, in  $\mathcal{F}\{\mathbb{Y}\}$  is a possibly infinitely generated ordinary algebraic ideal satisfying  $\sigma(\mathcal{I}) \subset \mathcal{I}$ . If  $S$  is a subset of  $\mathcal{F}\{\mathbb{Y}\}$ , we use  $(S)$  and  $[S]$  to denote the algebraic ideal and the  $\sigma$ -ideal generated by  $S$ .

A monomial order in  $\mathcal{F}\{\mathbb{Y}\}$  is called *compatible* with the  $\sigma$ -structure, if  $y_i^{x^{k_1}} < y_j^{x^{k_2}}$  for  $k_1 < k_2$ . Only compatible monomial orders are considered in this paper. When a monomial order is given, we use  $\mathbf{LM}(P)$  and  $\mathbf{LC}(P)$  to denote the largest monomial and its coefficient in  $P$  respectively, and  $\mathbf{LT}(P) = \mathbf{LC}(P)\mathbf{LM}(P)$  the leading term of  $P$ .

**Definition 2.1.**  $\mathbb{G} \subset \mathcal{F}\{\mathbb{Y}\}$  is called a  $\sigma$ -Gröbner basis of a  $\sigma$ -ideal  $\mathcal{I}$  if for any  $P \in \mathcal{I}$ , there exist  $m \in \mathbb{N}$  and  $G \in \mathbb{G}$  such that  $(\mathbf{LM}(G))^{x^m} \mid \mathbf{LM}(P)$ .

From the definition,  $\mathbb{G}$  is a  $\sigma$ -Gröbner basis of  $\mathcal{I}$  if and only if  $\Theta(\mathbb{G})$  is a Gröbner basis of  $\mathcal{I}$  treated as an algebraic polynomial ideal in  $\mathcal{F}[\Theta(\mathbb{Y})]$ . Note that  $\mathcal{I}$  is generally an infinitely generated ideal and the concept of infinite Gröbner basis [12] is adopted here. From this observation, we may see that a  $\sigma$ -Gröbner basis satisfies most of the properties of the usual algebraic Gröbner basis. For instance,  $\mathbb{G}$  is a  $\sigma$ -Gröbner basis of a  $\sigma$ -ideal  $\mathcal{I}$  if and only if for any  $P \in \mathcal{I}$ , we have  $\text{grem}(P, \Theta(\mathbb{G})) = 0$ , where  $\text{grem}(P, \Theta(\mathbb{G}))$  is the normal form of  $P$  modulo  $\Theta(\mathbb{G})$  in the theory of Gröbner basis. The concepts of reduced  $\sigma$ -Gröbner bases could be similarly introduced. A  $\sigma$ -polynomial  $Q$  is called  $\sigma$ -reduced w.r.t. another  $\sigma$ -polynomial  $P$  if there does not exist a  $k \in \mathbb{N}$  such that  $\mathbf{LM}(P)^{x^k}$  divides any monomial in  $Q$ . Then, a  $\sigma$ -Gröbner  $\mathbb{G}$  basis is called reduced, if any  $P \in \mathbb{G}$  is  $\sigma$ -reduced w.r.t.  $\mathbb{G} \setminus \{P\}$ . It is easy to see that a  $\sigma$ -ideal has a unique reduced  $\sigma$ -Gröbner basis.

The following example shows that even a finitely generated  $\sigma$ -ideal may have an infinite  $\sigma$ -Gröbner basis. As a consequence, there exist no general algorithms to compute the  $\sigma$ -Gröbner basis.

**Example 2.2.** Let  $\mathcal{I} = [y_1 y_2^x - y_1^x y_2, y_1 y_3 - 1]$ . Assume  $y_1 < y_2 < y_3$ . Then under a compatible monomial order, the reduced  $\sigma$ -Gröbner basis of  $\mathcal{I} \cap \mathcal{F}\{y_1, y_2\}$  is  $\{y_1 y_2^x - y_1^x y_2 \mid i \in \mathbb{N}_{>0}\}$ .

## 2.2 Characteristic set for a difference polynomial ideal

The *elimination ranking*  $\mathcal{R}$  on  $\Theta(\mathbb{Y}) = \{\sigma^k y_i \mid 1 \leq i \leq n, k \in \mathbb{N}\}$  is used in this paper:  $\sigma^k y_i > \sigma^l y_j$  if and only if  $i > j$  or  $i = j$  and  $k > l$ , which is a total order over  $\Theta(\mathbb{Y})$ . By convention,  $1 < \sigma^k y_j$  for all  $k \in \mathbb{N}$ .

Let  $f$  be a  $\sigma$ -polynomial in  $\mathcal{F}\{\mathbb{Y}\}$ . The greatest  $y_j^{x^k}$  w.r.t.  $\mathcal{R}$  which appears effectively in  $f$  is called the *leader* of  $f$ , denoted by  $\text{ld}(f)$  and correspondingly  $y_j$  is called the *leading variable* of  $f$ , denoted by  $\text{lvar}(f) = y_j$ . The leading coefficient of  $f$  as a univariate polynomial in  $\text{ld}(f)$  is called the *initial* of  $f$  and is denoted by  $\text{init}_f$ .

Let  $p$  and  $q$  be two  $\sigma$ -polynomials in  $\mathcal{F}\{\mathbb{Y}\}$ .  $q$  is said to be of higher rank than  $p$  if  $\text{ld}(q) > \text{ld}(p)$  or  $\text{ld}(q) = \text{ld}(p) = y_j^{x^k}$  and  $\deg(q, y_j^{x^k}) > \deg(p, y_j^{x^k})$ . Suppose  $\text{ld}(p) = y_j^{x^k}$ .  $q$  is said to be *Ritt-reduced* w.r.t.  $p$  if  $\deg(q, y_j^{x^{k+l}}) < \deg(p, y_j^{x^k})$  for all  $l \in \mathbb{N}$ .

A finite sequence of nonzero  $\sigma$ -polynomials  $\mathcal{A} : A_1, \dots, A_m$  is said to be a *difference ascending chain*, or simply a  $\sigma$ -chain, if  $m = 1$  and  $A_1 \neq 0$  or  $m > 1$ ,  $A_j > A_i$  and  $A_j$  is Ritt-reduced w.r.t.  $A_i$  for  $1 \leq i < j \leq m$ . A  $\sigma$ -chain  $\mathcal{A}$  can be written as the following form [8]

$$\mathcal{A} : A_{11}, \dots, A_{1k_1}, \dots, A_{p1}, \dots, A_{pk_p} \quad (1)$$

where  $\text{lvar}(A_{ij}) = y_{c_i}$  for  $j = 1, \dots, k_i$ ,  $\text{ord}(A_{ij}, y_{c_i}) < \text{ord}(A_{il}, y_{c_i})$  and  $\deg(A_{ij}, \text{ld}(A_{ij})) > \deg(A_{il}, \text{ld}(A_{il}))$  for

$j < l$ . The following are two  $\sigma$ -chains

$$\begin{aligned}\mathcal{A}_1 &: y_1^x - 1, \quad y_1^2 y_2^2 - 1, \quad y_2^x - 1 \\ \mathcal{A}_2 &: y_1^2 - 1, \quad y_1^x - y_1, \quad y_2^2 - 1, \quad y_2^x + y_2\end{aligned}\tag{2}$$

Let  $\mathcal{A} : A_1, A_2, \dots, A_t$  be a  $\sigma$ -chain with  $I_i$  as the initial of  $A_i$ , and  $P$  any  $\sigma$ -polynomial. Then there exists an algorithm, which reduces  $P$  w.r.t.  $\mathcal{A}$  to a  $\sigma$ -polynomial  $R$  that is Ritt-reduced w.r.t.  $\mathcal{A}$  and satisfies the relation

$$\prod_{i=1}^t I_i^{e_i} \cdot P \equiv R, \text{ mod } [\mathcal{A}],\tag{3}$$

where the  $e_i \in \mathbb{N}[x]$  and  $R = \text{prem}(P, \mathcal{A})$  is called the  $\sigma$ -Ritt-remainder of  $P$  w.r.t.  $\mathcal{A}$  [8].

A  $\sigma$ -chain  $\mathcal{C}$  contained in a  $\sigma$ -polynomial set  $\mathcal{S}$  is said to be a *characteristic set* of  $\mathcal{S}$ , if  $\mathcal{S}$  does not contain any nonzero element Ritt-reduced w.r.t.  $\mathcal{C}$ . Any  $\sigma$ -polynomial set has a characteristic set. A characteristic set  $\mathcal{C}$  of a  $\sigma$ -ideal  $\mathcal{J}$  reduces to zero all elements of  $\mathcal{J}$ .

Let  $\mathcal{A} : A_1, \dots, A_t$  be a  $\sigma$ -chain,  $I_i = \text{init}(A_i)$ ,  $y_{l_i}^{x^{o_i}} = \text{ld}(A_i)$ .  $\mathcal{A}$  is called *regular* if for any  $j \in \mathbb{N}$ ,  $I_i^{x^j}$  is invertible w.r.t.  $\mathcal{A}$  [8] in the sense that  $[A_1, \dots, A_{i-1}, I_i^{x^j}]$  contains a nonzero  $\sigma$ -polynomial involving no  $y_{l_i}^{x^{o_i+k}}$ ,  $k = 0, 1, \dots$ . To introduce the concept of coherent  $\sigma$ -chain, we need to define the  $\Delta$ -polynomial first. If  $A_i$  and  $A_j$  have distinct leading variables, we define  $\Delta(A_i, A_j) = 0$ . If  $A_i$  and  $A_j$  ( $i < j$ ) have the same leading variable  $y_l$ ,  $\text{ld}(A_i) = y_l^{x^{o_i}}$ , and  $\text{ld}(A_j) = y_l^{x^{o_j}}$ , then  $o_i < o_j$  [8]. Define  $\Delta(A_i, A_j) = \text{prem}((A_i)^{x^{o_j - o_i}}, A_j)$ . Then  $\mathcal{A}$  is called *coherent* if  $\text{prem}(\Delta(A_i, A_j), \mathcal{A}) = 0$  for all  $i < j$  [8]. Both  $\mathcal{A}_1$  and  $\mathcal{A}_2$  in (2) are regular and coherent  $\sigma$ -chains.

Let  $\mathcal{A}$  be a  $\sigma$ -chain. Denote  $\mathbb{I}_{\mathcal{A}}$  to be the minimal multiplicative set containing the initials of elements of  $\mathcal{A}$  and their transforms. The *saturation ideal* of  $\mathcal{A}$  is defined to be

$$\text{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbb{I}_{\mathcal{A}} = \{P \in \mathcal{F}\{\mathbb{Y}\} : \exists m \in \mathbb{I}_{\mathcal{A}}, mP \in [\mathcal{A}]\}.$$

The following result is needed in this paper.

**Theorem 2.3.** [8, Theorem 3.3] *A  $\sigma$ -chain  $\mathcal{A}$  is a characteristic set of  $\text{sat}(\mathcal{A})$  if and only if  $\mathcal{A}$  is regular and coherent.*

We also need the concept of algebraic saturation ideal. Let  $\mathcal{C}$  be an algebraic triangular set in  $\mathcal{F}[x_1, \dots, x_n]$  and  $I$  the product of the initials of the polynomials in  $\mathcal{C}$ . Then define

$$\text{asat}(\mathcal{C}) = \{P \in \mathcal{F}[x_1, \dots, x_n] \mid \exists k \in \mathbb{N}, I^k P \in (\mathcal{C})\}.$$

### 2.3 $\sigma$ -Gröbner basis for a binomial $\sigma$ -ideal

A  $\sigma$ -monomial in  $\mathbb{Y}$  can be written as  $\mathbb{Y}^{\mathbf{f}} = \prod_{i=1}^n y_i^{f_i}$ , where  $\mathbf{f} = (f_1, \dots, f_n)^{\tau} \in \mathbb{N}[x]^n$ . A nonzero vector  $\mathbf{f} = (f_1, \dots, f_n)^{\tau} \in \mathbb{Z}[x]^n$  is said to be *normal* if the leading coefficient of  $f_s$  is positive, where  $s$  is the largest subscript such that  $f_s \neq 0$ . For  $\mathbf{f} \in \mathbb{Z}[x]^n$ , let  $\mathbf{f}^+, \mathbf{f}^- \in \mathbb{N}^n[x]$  denote respectively the positive part and the negative part of  $\mathbf{f}$  such that  $\mathbf{f} = \mathbf{f}^+ - \mathbf{f}^-$ . Then  $\gcd(\mathbb{Y}^{\mathbf{f}^+}, \mathbb{Y}^{\mathbf{f}^-}) = 1$  for any  $\mathbf{f} \in \mathbb{Z}[x]^n$ . If  $\mathbf{f} \in \mathbb{Z}[x]^n$  is normal, then  $\mathbb{Y}^{\mathbf{f}^+} > \mathbb{Y}^{\mathbf{f}^-}$  and  $\mathbf{LT}(\mathbb{Y}^{\mathbf{f}^+} - c\mathbb{Y}^{\mathbf{f}^-}) = \mathbb{Y}^{\mathbf{f}^+}$  under a monomial order compatible with the  $\sigma$ -structure.

A  $\sigma$ -binomial in  $\mathbb{Y}$  is a  $\sigma$ -polynomial with at most two terms, that is,  $a\mathbb{Y}^{\mathbf{a}} + b\mathbb{Y}^{\mathbf{b}}$  where  $a, b \in \mathcal{F}$  and  $\mathbf{a}, \mathbf{b} \in \mathbb{N}[x]^n$ . A  $\sigma$ -ideal in  $\mathcal{F}\{\mathbb{Y}\}$  is called *binomial* if it is generated by, possibly infinitely many,  $\sigma$ -binomials [7]. We have

**Proposition 2.4** ([7]). A  $\sigma$ -ideal  $\mathcal{J}$  is binomial if and only if the reduced  $\sigma$ -Gröbner basis for  $\mathcal{J}$  consists of  $\sigma$ -binomials.

Let  $\mathfrak{m}$  be the multiplicative set generated by  $y_i^{x_j}$  for  $i = 1, \dots, n, j \in \mathbb{N}$ . A  $\sigma$ -ideal  $\mathcal{J}$  is called *normal* if for  $M \in \mathfrak{m}$  and  $P \in \mathcal{J} \setminus \{0\}$ ,  $MP \in \mathcal{J}$  implies  $P \in \mathcal{J}$ . Normal  $\sigma$ -ideals in  $\mathcal{F}\{\mathbb{Y}\}$  are closely related with the  $\mathbb{Z}[x]$ -modules in  $\mathbb{Z}[x]^n$  [7, 13], which will be explained below. We first introduce a new concept.

**Definition 2.5.** A partial character  $\rho$  on  $\mathbb{Z}[x]^n$  is a homomorphism from a  $\mathbb{Z}[x]$ -module  $L_\rho$  in  $\mathbb{Z}[x]^n$  to the multiplicative group  $\mathcal{F}^*$  satisfying  $\rho(x\mathbf{f}) = (\rho(\mathbf{f}))^x = \sigma(\rho(\mathbf{f}))$  for  $\mathbf{f} \in L_\rho$ .

A  $\mathbb{Z}[x]$ -module generated by  $\mathbf{h}_1, \dots, \mathbf{h}_m \in \mathbb{Z}[x]^n$  is denoted as  $(\mathbf{h}_1, \dots, \mathbf{h}_m)_{\mathbb{Z}[x]}$ . Let  $\rho$  be a partial character over  $\mathbb{Z}[x]^n$  and  $\mathbf{f} = \{\mathbf{f}_1, \dots, \mathbf{f}_s\}$  a reduced Gröbner basis of the  $\mathbb{Z}[x]$ -module  $L_\rho = (\mathbf{f})_{\mathbb{Z}[x]}$ . For  $\mathbf{h} \in \mathbb{Z}[x]^n$  and  $H \subset L_\rho$ , denote  $\mathbb{P}_{\mathbf{h}} = \mathbb{Y}^{\mathbf{h}^+} - \rho(\mathbf{h})\mathbb{Y}^{\mathbf{h}^-}$  and  $\mathbb{P}_H = \{\mathbb{P}_{\mathbf{h}} \mid \mathbf{h} \in H\}$ . Introduce the following notations associated with  $\rho$ :

$$\mathcal{J}^+(\rho) := [\mathbb{P}_{L_\rho}] = [\mathbb{Y}^{\mathbf{f}^+} - \rho(\mathbf{f})\mathbb{Y}^{\mathbf{f}^-} \mid \mathbf{f} \in L_\rho] \quad (4)$$

$$\mathcal{A}^+(\rho) := \mathbb{P}_{\mathbf{f}} = \{\mathbb{Y}^{\mathbf{f}_1^+} - \rho(\mathbf{f}_1)\mathbb{Y}^{\mathbf{f}_1^-}, \dots, \mathbb{Y}^{\mathbf{f}_s^+} - \rho(\mathbf{f}_s)\mathbb{Y}^{\mathbf{f}_s^-}\}. \quad (5)$$

It is shown that [7]  $\mathcal{A}^+(\rho)$  is a regular and coherent  $\sigma$ -chain and hence is a characteristic set of  $\text{sat}(\mathcal{A}^+(\rho))$  by Theorem 2.3. Furthermore, we have

**Theorem 2.6.** The following conditions are equivalent.

1.  $\mathcal{J}$  is a normal binomial  $\sigma$ -ideal in  $\mathcal{F}\{\mathbb{Y}\}$ .
2.  $\mathcal{J} = \mathcal{J}^+(\rho)$  for a partial character  $\rho$  over  $\mathbb{Z}[x]^n$ .
3.  $\mathcal{J} = \text{sat}(\mathcal{A}^+(\rho))$  for a partial character  $\rho$  over  $\mathbb{Z}[x]^n$ .

Furthermore, for  $\mathbf{f} \in \mathbb{Z}[x]^n$ ,  $\mathbb{Y}^{\mathbf{f}^+} - c\mathbb{Y}^{\mathbf{f}^-} \in \mathcal{J} \Leftrightarrow \mathbf{f} \in L_\rho$  and  $c = \rho(\mathbf{f})$ .

As a direct consequence of Proposition 2.4 and Theorem 2.6, we have

**Corollary 2.7.** Let  $\rho$  be a partial character over  $\mathbb{Z}[x]^n$ . Then  $\mathbb{P}_{L_\rho}$  is a  $\sigma$ -Gröbner basis of  $\mathcal{J}^+(\rho)$ .

Note that for  $\mathbf{f} \in \mathbb{Z}[x]^n$ , either  $\mathbf{f}$  or  $-\mathbf{f}$  is normal and we need only consider the normal vectors in the  $\sigma$ -Gröbner basis. So, for simplicity, we may assume that all given vectors are normal. We have the following criterion for the  $\sigma$ -Gröbner basis of normal binomial  $\sigma$ -ideals.

**Corollary 2.8.** Let  $\rho$  be a partial character over  $\mathbb{Z}[x]^n$  and  $H \subset L_\rho$ . Then  $\mathbb{P}_H$  is a  $\sigma$ -Gröbner basis of  $\mathcal{J}^+(\rho)$  if and only if for any normal  $\mathbf{g} \in L_\rho$ , there exist  $\mathbf{h} \in H$  and  $j \in \mathbb{N}$ , such that  $\mathbf{g}^+ - x^j\mathbf{h}^+ \in \mathbb{N}[x]^n$ .

*Proof:* By Corollary 2.7,  $\mathbb{P}_{L_\rho}$  is a  $\sigma$ -Gröbner basis of  $\mathcal{J}^+(\rho)$ . Then  $\mathbb{P}_H$  is a  $\sigma$ -Gröbner basis of  $\mathcal{J}^+(\rho)$  if and only if for any normal  $\mathbf{g} \in L_\rho$ , there exist  $\mathbf{h} \in H$  and  $j \in \mathbb{N}$  such that  $\mathbf{LM}(x^j\mathbb{P}_{\mathbf{h}}) \mid \mathbf{LM}(\mathbb{P}_{\mathbf{g}})$ , which is equivalent to  $\mathbf{g}^+ - x^j\mathbf{h}^+ \in \mathbb{N}[x]^n$ .

**Example 2.9.** Let  $\mathbf{f} = [1 - x, x - 1]$ ,  $L = (\mathbf{f})_{\mathbb{Z}[x]}$ , and  $\rho$  the trivial partial character on  $L$ , that is,  $\rho(\mathbf{h}) = 1$  for  $\mathbf{h} \in L$ . Then  $\mathbb{P}_{\mathbf{f}} = y_1y_2^x - y_1^xy_2$ . By Theorem 2.6,  $\mathcal{J}^+(\rho) = \text{sat}(\mathbb{P}_{\mathbf{f}})$ . By Corollary 2.7, a  $\sigma$ -Gröbner basis of  $\mathcal{J}^+(\rho)$  is  $\{\mathbb{Y}^{\mathbf{g}^+} - \mathbb{Y}^{\mathbf{g}^-} \mid \mathbf{g} = h\mathbf{f}, h \in \mathbb{Z}[x], \text{lc}(h) > 0\}$ . By Example 2.2,  $\text{sat}(\mathbb{P}_{\mathbf{f}}) = [\mathbb{P}_{\mathbf{f}}, y_1y_2 - 1] \cap \mathbb{Q}\{y_1, y_2\} = [y_1y_2^x - y_1^xy_2 \mid i \in \mathbb{N}_{>0}]$ , and a reduced  $\sigma$ -Gröbner basis of  $\mathcal{J}^+(\rho)$  is  $\{y_1y_2^x - y_1^xy_2 \mid i \in \mathbb{N}_{>0}\}$ .

### 3 Criteria for finite $\sigma$ -Gröbner basis

In this section, we will give a criterion for the  $\sigma$ -Gröbner basis of a normal binomial  $\sigma$ -ideal in  $\mathcal{F}\{y\}$  to be finite, where  $y$  is a  $\sigma$ -indeterminate. Without loss of generality, we assume  $\rho(h) = 1$  for all partial characters  $\rho$  over  $\mathbb{Z}[x]$  and  $h \in L_\rho$ .

#### 3.1 Case 1: characteristic set contains a single $\sigma$ -polynomial

In this section, we consider the simplest case:  $n = 1$  and  $L_\rho = (f)_{\mathbb{Z}[x]}$  is generated by one polynomial  $f \in \mathbb{Z}[x]$ . We will see that even this case is highly nontrivial. For  $g \in \mathbb{Z}[x]$ , we use  $\text{lc}(g)$ ,  $\text{lm}(g)$ , and  $\text{lt}(g)$  to represent the leading coefficient, leading monomial, and leading term of  $g$ , respectively.

In the rest of this section, we assume  $f \in \mathbb{Z}[x]$  and  $\text{lc}(f) > 0$ . Then  $\mathbb{P}_f = y^{f^+} - y^{f^-}$  and  $\mathbf{LT}(\mathbb{P}_f) = y^{f^+}$  under a monomial order compatible with the  $\sigma$ -structure. By Theorem 2.6, all normal binomial  $\sigma$ -ideals in  $\mathcal{F}\{y\}$  whose characteristic set consists of a single  $\sigma$ -polynomial can be written as the following form:

$$\mathcal{I}_f = \text{sat}(\mathbb{P}_f) = [y^{h^+} - y^{h^-} \mid h = fg \in (f)_{\mathbb{Z}[x]}, \forall (g \in \mathbb{Z}[x], \text{lc}(g) > 0)]. \quad (6)$$

In this section, we will give a criterion for  $\mathcal{I}_f$  to have a finite  $\sigma$ -Gröbner basis. Define

$$\begin{aligned} \Phi_0 &\triangleq \{f \in \mathbb{Z}[x] \mid \text{lt}(f) = f^+\}. \\ \Phi_1 &\triangleq \{f \in \mathbb{Z}[x] \mid fg \in \Phi_0 \text{ for some monic polynomial } g \in \mathbb{Z}[x]\}. \end{aligned} \quad (7)$$

We now give the main result of this section, which can be deduced from Lemma 3.3 and Lemma 3.7.

**Theorem 3.1.**  $\mathcal{I}_f$  in (6) has a finite  $\sigma$ -Gröbner basis under a monomial order compatible w.r.t the  $\sigma$ -structure if and only if  $f \in \Phi_1$ .

For two polynomials  $h_1$  and  $h_2 \in \mathbb{Z}[x]$ , denote  $h_1 \succeq h_2$  if  $h_1 - h_2 \in \mathbb{N}[x]$ . For  $h_1$  and  $h_2 \in \mathbb{N}[x]$ , we have  $h_1 \succeq h_2$  if and only if  $y^{h_2} \mid y^{h_1}$ .

**Lemma 3.2.** If  $f \in \Phi_0$ , then  $\{\mathbb{P}_f\}$  is a  $\sigma$ -Gröbner basis of  $\mathcal{I}_f$ .

*Proof:* For  $g \in (f)_{\mathbb{Z}[x]}$  with  $\text{lc}(g) > 0$ ,  $\exists h \in \mathbb{Z}[x]$  with  $\text{lc}(h) > 0$  such that  $g = fh$ . Since  $f \in \Phi_0$ , we have  $\text{lt}(f) = f^+$ . Then,

$$x^{\deg(h)} f^+ = \text{lt}(h) f^+ / \text{lc}(h) \preceq \text{lt}(h) f^+ = \text{lt}(h) \text{lt}(f) = \text{lt}(g) \preceq g^+.$$

By Corollary 2.8,  $\{\mathbb{P}_f\}$  is a  $\sigma$ -Gröbner basis of  $\mathcal{I}_f$ .

**Lemma 3.3.** If  $f \in \Phi_1$ , then  $\mathcal{I}_f$  has a finite  $\sigma$ -Gröbner basis.

*Proof:* Let  $h = fg \in \Phi_0$ , where  $g$  is monic. Then  $\text{lc}(h) = \text{lc}(f)$  and  $\text{lt}(h) = \text{lt}(f) \text{lm}(g) = h^+$ .  $\mathcal{I}_{\deg(h)} = \mathcal{I}_f \cap \mathcal{F}[y, y^x, \dots, y^{x^{\deg(h)}}]$  is a polynomial ideal in a polynomial ring with finitely many variables, which has a finite Gröbner basis denoted by  $\mathbb{G}_{\leq \deg(h)}$ . Let  $\mathbb{P}_u \in \mathcal{I}_f$  and  $\text{lc}(u) > 0$ . If  $\deg(u) \leq \deg(h)$ , then there exists a  $\mathbb{P}_t \in \mathbb{G}_{\leq \deg(h)}$  such that  $t \preceq u$ . Otherwise, we have  $\deg(u) > \deg(h)$  and  $\text{lc}(u) \geq \text{lc}(f)$ . Then

$$\begin{aligned} x^{\deg(u) - \deg(h)} h^+ &= x^{\deg(u) - \deg(f) - \deg(g)} \text{lt}(f) \text{lm}(g) \\ &= x^{\deg(u) - \deg(f)} \text{lt}(f) = x^{\deg(u) - \deg(f)} \text{lc}(f) \text{lm}(f) = \text{lc}(f) \text{lm}(u) \preceq \text{lt}(u) \preceq u^+. \end{aligned}$$

Since that  $\mathbb{P}_h \in \mathcal{I}_{\deg(h)}$ , by Corollary 2.8,  $\mathbb{G}_{\leq \deg(s)}$  is a finite  $\sigma$ -Gröbner basis of  $\mathcal{I}_f$ .

**Corollary 3.4.** Let  $f \in \Phi_1$ ,  $h = gf \in \Phi_0$ ,  $g$  a monic polynomial in  $\mathbb{Z}[x]$ , and  $D = \deg(h)$ . Then the Gröbner basis of the polynomial ideal  $\mathcal{I}_D = \mathcal{I}_f \cap \mathcal{P}[y, y^x, \dots, y^{x^D}]$  is a finite  $\sigma$ -Gröbner basis for  $\mathcal{I}_f$ .

From the proof of Lemma 3.3, we have

**Example 3.5.**  $f = x^2 + x + 1 \in \Phi_1$ , because  $(x-1)f = x^3 - 1 \in \Phi_0$ . The finite  $\sigma$ -Gröbner basis is  $\mathbb{G} = \{y^{x^2+x+1} - 1, y^{x^3} - y\}$ .

Let  $D$  be  $\mathbb{R}$  or  $\mathbb{Z}$ . We will use the following new notation

$$D^{>0}[x] \triangleq \left\{ \sum_{i=0}^n a_i x^i \mid n \in \mathbb{N}, \forall i (a_i \in D_{>0}) \right\}.$$

**Lemma 3.6.**  $\mathbb{N}[x] \subseteq \Phi_1$ .

*Proof:* Let  $g = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{N}[x]$  with  $d = \max\{d \in \mathbb{N} \mid x^d \mid g\}$  the multiplicity of  $f$  at 0. Then  $a_d > 0$ . Let  $s = (x^{n-d} + x^{n-d-1} + \dots + 1)g = a_n x^{2n-d} + (a_n + a_{n-1})x^{2n-d-1} + \dots + (a_n + \dots + a_d)x^n + (a_{n-1} + \dots + a_d)x^{n-1} + \dots + a_d x^d$ . Rewrite  $s = b_{2n-d} x^{2n-d} + \dots + b_d x^d$ . Then  $s/x^d \in \mathbb{Z}^{>0}[x]$ . Let  $M = \lceil \max\{b_{i-1}/b_i \mid d+1 \leq i \leq 2n-d\} \rceil + 1$ . Then  $(x-M)s = b_{2n-d} x^{2n-d+1} + (b_{2n-d-1} - Mb_{2n-d})x^{2n-d} + \dots + (b_d - Mb_{d+1})x^{d+1} - Mb_d x^d \in \Phi_0$ . So both  $s$  and  $g$  are in  $\Phi_1$ .

**Lemma 3.7.** If  $f \notin \Phi_1$ , then  $\mathcal{I}_f$  does not have a finite  $\sigma$ -Gröbner basis.

*Proof:* Suppose otherwise,  $\mathcal{I}_f$  has a finite  $\sigma$ -Gröbner basis  $\mathbb{G} = \mathbb{P}_H$ , where  $H = \{f_1, \dots, f_l\} \subset \mathbb{Z}[x]$  with each  $\text{lc}(f_i) > 0$ . Since  $f$  has the lowest degree in  $(f)_{\mathbb{Z}[x]}$ , we have  $f \in H$ .

Let  $H_c \triangleq \{h \in H \mid \text{lc}(h) = \text{lc}(f)\}$ . Since  $f \notin \Phi_1$ , we have  $H_c \cap \Phi_1 = \emptyset$ . By Lemmas 3.2 and 3.6, for all  $h \in H_c$ ,  $h^+$  has at least two terms and  $h^-$  has at least one term. For  $u \in \mathbb{Z}[x]$  with  $\text{lc}(u) > 0$ , define a function

$$\widetilde{\deg}(u) = \deg(u) - (\deg(u^+) - \text{lt}(u)) \quad (8)$$

which is the degree gap between the first two highest monomials of  $u^+$ . Suppose  $h_1$  is an element in  $H_c$  such that  $\widetilde{\deg}(h_1) = \max\{\widetilde{\deg}(h) \mid h \in H_c\}$ .  $h_1$  exists because  $f \in H_c \neq \emptyset$  and  $H_c$  is a finite set. Denote  $\text{lt}(h_1) \triangleq ax^n$ ,  $\tilde{h}_1 \triangleq h_1 - \text{lt}(h_1)$ ,  $\text{lt}(\tilde{h}_1^+) \triangleq bx^m$ , and  $\tilde{\tilde{h}}_1^+ \triangleq \tilde{h}_1^+ - \text{lt}(\tilde{h}_1^+)$ . Then  $h_1 = ax^n + bx^m + \tilde{\tilde{h}}_1^+ - h_1^-$ . Since  $h_1 \notin \Phi_1$ , we have  $ab > 0$ . Let  $c \triangleq \lceil b/a \rceil \geq 1$  and

$$s = (x^n - cx^m)h_1 = ax^{2n} + x^n \tilde{\tilde{h}}_1^+ + cx^m h_1^- - (ac - b)x^{m+n} - cx^m \tilde{\tilde{h}}_1^+ - x^n h_1^-.$$

We have  $s^+ \preceq s_0 \triangleq ax^{2n} + x^n \tilde{\tilde{h}}_1^+ + cx^m h_1^-$ , and  $\widetilde{\deg}(s) = \deg(s) - \deg(s^+ - \text{lt}(s)) \geq \widetilde{\deg}(s_0) = \deg(s_0) - \deg(s_0^+ - \text{lt}(s_0)) > n - m = \widetilde{\deg}(h_1) = \deg(h_1) - \deg(h_1^+ - \text{lt}(h_1))$ .

Since  $\mathbb{P}_H$  is a  $\sigma$ -Gröbner basis of  $\mathcal{I}_f$ , there exist  $h \in H$  and  $j \in \mathbb{N}$  such that  $t = s^+ - x^j h^+ \in \mathbb{N}[x]$ . We claim  $\text{lt}(t) = \text{lt}(s^+)$ . If  $h \in H_c$ , then  $\widetilde{\deg}(s) > \widetilde{\deg}(h)$ . Note that  $\deg(s^+) = \deg(x^j h)$  implies that the coefficient of the second largest monomial of  $s^+ - x^j h$  is negative contradicting to the fact  $s^+ - x^j h \in \mathbb{N}[x]$ . As a consequence, we must have  $\deg(s^+) > \deg(x^j h)$  and the claim is proved in this case. Now let  $h \in H \setminus H_c$ . Since  $\text{lc}(h) > \text{lc}(s) = \text{lc}(f)$ , we have  $\deg(x^j h) < \deg(s)$  which implies  $\text{lt}(t) = \text{lt}(s^+)$ . The claim is proved. The fact  $\text{lt}(t) = \text{lt}(s^+)$  implies that when computing the normal form  $\mathbb{P}_u = \text{grem}(\mathbb{P}_s, \Theta(\mathbb{P}_H))$ , we always have  $\text{lt}(u) = \text{lt}(s)$ . As a consequence,  $\mathbb{P}_u \neq 0$  which contradicts to the fact that  $\mathbb{P}_H$  is a  $\sigma$ -Gröbner basis of  $\mathcal{I}_f$  and  $s \in (f)_{\mathbb{Z}[x]}$ .

Note that the proof of Lemma 3.7 gives a method to construct infinitely many elements in a  $\sigma$ -Gröbner basis as shown in the following example.

**Example 3.8.** Let  $f = x^2 - 2x + 1 \notin \Phi_1$ . In the proof of Lemma 3.7,  $c = \lceil b/a \rceil = 1$  and  $s_1 = (x^2 - 1)f = x^4 + 2x - 2x^3 - 1$ . Repeat the above procedure to  $s_1$ , we obtain  $s_2 = (x^4 - 2x)s_1 = x^8 + 3x^4 + 2x - 2x^7 - 4x^2$ . Then  $\widetilde{\deg}(f) < \widetilde{\deg}(s_1) < \widetilde{\deg}(s_2)$  and  $\mathbb{P}_{s_i}$  is in a  $\sigma$ -Gröbner basis for all  $i$ . Thus any  $\sigma$ -Gröbner basis of  $\mathcal{J}_f$  is infinite. We can show that a minimal  $\sigma$ -Gröbner basis is  $\mathbb{G} = \{y^{x^{2i}+1} - y^{2x^i} \mid i \in \mathbb{Z}_{>0}\} \cup \{y^{x^{2i+1}+1} - y^{x^{i+1}+x^i} \mid i \in \mathbb{Z}_{>0}\}$ .

### 3.2 Finite $\sigma$ -Gröbner bases for normal binomial $\sigma$ -ideals

In this section, we consider the general normal binomial  $\sigma$ -ideals in  $\mathcal{F}\{y\}$ . By Theorem 2.6, all normal binomial  $\sigma$ -ideals in  $\mathcal{F}\{y\}$  can be written as the following form:

$$\mathcal{J}_{\mathbb{G}} = \text{sat}(\mathbb{P}_{\mathbb{G}}) = [y^{g^+} - y^{g^-} \mid \forall g \in (\mathbb{G})_{\mathbb{Z}[x]}, \text{lc}(g) > 0] \quad (9)$$

where

$$\mathbb{G} = \{g_1, \dots, g_t\} \subset \mathbb{Z}[x] \quad (10)$$

is a reduced Gröbner basis of the  $\mathbb{Z}[x]$ -module  $L = (\mathbb{G})_{\mathbb{Z}[x]}$ . Gröbner bases in  $\mathbb{Z}[x]$  have the following special structure [7].

**Lemma 3.9.** Let  $\mathbb{G} = \{g_1, \dots, g_k\}$  be a reduced Gröbner basis of a  $\mathbb{Z}[x]$ -module in  $\mathbb{Z}[x]$ ,  $g_1 < \dots < g_k$ , and  $\text{lt}(g_i) = c_i x^{d_i} \in \mathbb{N}[x]$ . Then

- 1)  $0 \leq d_1 < d_2 < \dots < d_k$ .
- 2)  $c_k \mid \dots \mid c_2 \mid c_1$  and  $c_i \neq c_{i+1}$  for  $1 \leq i \leq k-1$ .
- 3)  $\frac{c_i}{c_k} \mid g_i$  for  $1 \leq i < k$ . If  $\widetilde{b}_1$  is the primitive part of  $g_1$ , then  $\widetilde{b}_1 \mid g_i$  for  $1 < i \leq k$ .

Here are two Gröbner bases in  $\mathbb{Z}[x]$ :  $\{4, 2x\}$ ,  $\{15, 5x, x^2 + 3\}$ .

In the rest of this section, let  $L = (\mathbb{G})_{\mathbb{Z}[x]}$  for  $\mathbb{G}$  defined in (10) and define

$$L_i \triangleq \{f \in L \mid \text{lc}(f) = c_i = \text{lc}(g_i)\} \quad (11)$$

$$L_t \triangleq \{f \in L_i \mid f \text{ has minimal degree in } L_i\}. \quad (12)$$

**Theorem 3.10.**  $\mathcal{J}_{\mathbb{G}}$  has a finite  $\sigma$ -Gröbner basis if and only if  $L_i \cap \Phi_0 \neq \emptyset$ .

*Proof:* Suppose  $L_i \cap \Phi_0 \neq \emptyset$  and let  $g \in L_i \cap \Phi_0$ . Then  $\mathcal{J}_{\mathbb{G}} \cap k[y, y^x, \dots, y^{x^{\deg(g)}}]$  has a finite Gröbner basis denoted by  $G_{\leq \deg(g)}$ . Let  $\mathbb{P}_u \in \mathcal{J}_{\mathbb{G}}$  and  $\text{lc}(u) > 0$ . If  $\deg(u) \leq \deg(g)$ , then there exists a  $\mathbb{P}_h \in G_{\leq \deg(g)}$  such that  $h \preceq u$ . Otherwise, we have  $\deg(u) > \deg(g)$  and  $\text{lc}(u) \geq \text{lc}(g)$ . Then

$$x^{\deg(u)-\deg(g)} g^+ = x^{\deg(u)-\deg(g)} \text{lt}(g) = x^{\deg(u)-\deg(g)} \text{lc}(g) \text{lm}(g) = \text{lc}(g) \text{lm}(u) \preceq \text{lt}(u) \preceq u^+.$$

By Corollary 2.8,  $\mathbb{G}_{\leq \deg(g)}$  is a finite  $\sigma$ -Gröbner basis of  $\mathcal{J}_{\mathbb{G}}$ , since  $\mathbb{P}_g$  is in  $\mathbb{G}_{\leq \deg(g)}$ .

We will prove the other direction by contradiction. Suppose that  $L_i \cap \Phi_0 = \emptyset$  and  $\mathcal{J}_{\mathbb{G}}$  has a finite  $\sigma$ -Gröbner basis  $\mathbb{P}_H = \{\mathbb{P}_{u_1}, \dots, \mathbb{P}_{u_k}\}$ . Let  $H = \{u_1, \dots, u_k\}$ , and  $H_c = H \cap L_i$ . Since  $\text{grem}(\mathbb{P}_g, \Theta(\mathbb{P}_H)) = 0$ , we have  $H_c \neq \emptyset$  and let  $u_1$  be an element of  $H_c$  with maximal  $\widetilde{\deg}$  which is defined in (8). Since  $L_i \cap \Phi_0 = \emptyset$ , by Lemma 3.6  $u_1^+$  contains at least two terms and  $u_1^- \neq 0$ . Similar to the proof of Lemma 3.7, we can construct an  $s \in \mathbb{Z}[x] \cap L$  such that  $\widetilde{\deg}(s) > \widetilde{\deg}(u_1)$  and  $\text{lc}(s) = \text{lc}(u_1)$ . Then,  $\text{grem}(\mathbb{P}_s, \Theta(\mathbb{P}_H)) \neq 0$  contradicting to the fact that  $\mathbb{P}_H$  is a  $\sigma$ -Gröbner basis.



**Corollary 3.11.** *If  $\mathcal{J}_{\mathbb{G}}$  has a finite  $\sigma$ -Gröbner basis, then  $g_1 \in \Phi_1$ .*

*Proof:* Let  $\tilde{b}_1$  be the primitive part of  $g_1$ . Then by Lemma 3.9,  $\tilde{b}_1 | h$  for any  $h \in L$ . By Theorem 3.10,  $\tilde{b}_1$  and hence  $g_1$  is in  $\Phi_1$ .

**Corollary 3.12.** *If  $L_t \cap \Phi_1 \neq \emptyset$  and in particular  $g_t \in \Phi_1$ , then  $\mathcal{J}_{\mathbb{G}}$  has finite  $\sigma$ -Gröbner Basis.*

The following example shows that  $g_t \in \Phi_1$  is not a necessary condition for the  $\sigma$ -Gröbner basis to be finite.

**Example 3.13.** *Let  $\mathbb{G} = \{2(x^2 - 2), (x^2 - 2)(x + 1)\}$ . Then  $(x^2 - 2)(x + 1)(x - 1) + 2(x^2 - 2) = x^4 - x^2 - 2 \in \Phi_0 \subset \Phi_1$ , and hence  $\mathcal{J}_{\mathbb{G}}$  has a finite  $\sigma$ -Gröbner basis. On the other hand, we will show  $(x^2 - 2)(x + 1) \notin \Phi_1$  in Example 4.10.*

In order to give another criterion, we need the following effective Polya Theorem.

**Lemma 3.14** ([17]). *Suppose that  $f(x) = \sum_{j=0}^n a_n x^n \in \mathbb{R}[x]$  is positive on  $[0, \infty)$  and  $F(x, y)$  the homogenization of  $f$ . Then for  $N_f > \frac{n(n-1)L}{2\lambda} - n$ ,  $(1+x)^{N_f} f(x) \in \mathbb{R}^{>0}[x]$ , where  $\lambda = \min\{F(x, 1-x) | x \in [0, 1]\}$  and  $L = \max\{\frac{k!(n-k)!}{n!} | a_k\}$ .*

**Corollary 3.15.** *If there exists an  $h \in L$  with no positive real roots, then  $\mathcal{J}_{\mathbb{G}}$  has a finite  $\sigma$ -Gröbner basis.*

*Proof:* Write  $h = x^{m_1} h_1$  such that  $h_1(0) \neq 0$ . By Lemma 3.14, there exists an  $N \in \mathbb{N}$  such that  $h_2 = (x+1)^N h \in \mathbb{Z}^{>0}[x]$ . Take a sufficiently large  $N$  such that  $\deg(h_2) > d_t = \deg(g_t)$ . Then there exists a sufficiently large  $M \in \mathbb{N}$ , such that  $\bar{g} = x^{m_1} (x^{\deg(h_2) - \deg(g_t) + 1} g_t - M h_2) \in \Phi_0$ . Since  $\bar{g} \in L_i$ , by Lemma 3.10,  $\mathcal{J}$  has a finite  $\sigma$ -Gröbner Basis.

## 4 Membership decision for $\Phi_1$ and $\sigma$ -Gröbner basis computation

In Section 3, we prove that  $\text{sat}(\mathbb{P}_f)$  has a finite  $\sigma$ -Gröbner basis if and only if  $f \in \Phi_1$ . In this section, we will give criteria and an algorithm for  $f \in \Phi_1$ . If  $f \in \Phi_1$ , we also give an algorithm to compute the finite  $\sigma$ -Gröbner basis.

From the definition of  $\Phi_1$ , a necessarily condition for  $f \in \Phi_1$  is  $\text{lc}(f) > 0$ . Also, it is easy to show that  $f \in \Phi_1$  if and only if  $c x^m f \in \Phi_1$  for positive integers  $c$  and  $m$ . So in the rest of this paper, we assume

$$f = \sum_{i=0}^n a_n x^i \in \mathbb{Z}[x]$$

such that  $n > 0$ ,  $\text{lc}(f) = a_n > 0$ ,  $f(0) = a_0 \neq 0$ , and  $\gcd(a_0, a_1, \dots, a_n) = 1$ .

### 4.1 Decision criteria

In this subsection, we will study whether  $f \in \Phi_1$  by examining properties of the roots of  $f(x) = 0$ .

**Lemma 4.1.** *If  $f \in \mathbb{Z}[x]$  has no positive real roots, then  $f \in \Phi_1$ .*

*Proof:* By Lemma 3.14, there exists an  $N \in \mathbb{N}$ , such that  $(x+1)^N f \in \mathbb{Z}^{>0}[x] \subseteq \mathbb{N}[x]$ . By Lemma 3.6,  $(x+1)^N f \in \mathbb{N}[x] \subseteq \Phi_1$ , and thus  $f \in \Phi_1$ .

By Lemma 4.1, we need only consider those polynomials which have positive roots.

**Lemma 4.2.** *Let  $f = a_n x^n + \dots + a_0 \in \Phi_0$ . Then  $f$  has a simple and unique positive real root  $x_+$ , and for any root  $z$  of  $f$ , we have  $|z| \leq x_+$ .*

*Proof:* Since  $f \in \Phi_0 \setminus \mathbb{Z}$ , the number of sign differences of  $f$  is one. Then by Descartes' rule of signs [1], the number of positive real roots of  $f$  (with multiplicities counted) is one or less than one by an even number. Then  $f$  has a simple and unique positive real root  $x_+$ . For any root  $z$  of  $f$ , since  $-a_i \geq 0$  for  $i = 0, \dots, n-1$ , we have

$$a_n |z|^n = |a_n z^n| = |-a_{n-1} z^{n-1} - \dots - a_0| \leq -a_{n-1} |z|^{n-1} - \dots - a_0. \quad (13)$$

Thus  $f(|z|) \leq 0$  and hence  $f$  has at least one real root in  $[|z|, \infty)$ . Since  $f$  has a unique positive real root  $x_+$ , we have  $|z| \leq x_+$ .

We now consider those  $f$  which has a root  $z \neq x_+$  and  $|z| = x_+$ . Such a  $z$  must be either  $-x_+$  or a complex root.

**Lemma 4.3.** *Let  $f = a_n x^n + \dots + a_0 \in \Phi_0$  and  $x_+$  the unique positive root of  $f$ . If  $f$  has a root  $z \neq x_+$  but  $|z| = x_+$ , then we have*

1.  $z^{\delta_f} \in \mathbb{R}_{>0}$  and  $z$  is a simple root of  $f$ , where  $\delta_f = \gcd\{i \mid a_i \neq 0\} > 1$ .
2.  $f$  is a polynomial in  $x^{\delta_f}$ :  $f = \hat{f} \circ x^{\delta_f}$ , where  $\circ$  is the function composition. Furthermore,  $\hat{f}(w) = 0$  and  $|w| = x_+^{\delta_f}$  imply  $w = x_+^{\delta_f}$ .
3.  $f$  has exactly  $\delta_f$  roots with absolute value  $x_+$ :  $\{z \mid f(z) = 0, |z| = x_+\} = \{\zeta^k x_+ \mid \zeta = e^{\frac{2\pi i}{\delta_f}}, k = 1, \dots, \delta_f\}$ , where  $\mathbf{i} = \sqrt{-1}$ .

*Proof:* Let  $z \neq x_+$  be a root of  $f$  such that  $|z| = x_+$ . Then  $f(|z|) = f(x_+) = a_n |z|^n + a_{n-1} |z|^{n-1} + \dots + a_0 = 0$ , which, combining with (13), implies  $|-a_{n-1} z^{n-1} - \dots - a_0| = -a_{n-1} |z|^{n-1} - \dots - a_0$ . The above equation is possible if and only if  $-a_i z^i \in \mathbb{R}_{>0}$  for each  $i \leq n-1$  and  $a_i \neq 0$ . Also note,  $z^n = (-a_{n-1} |z|^{n-1} - \dots - a_0)/a_n \in \mathbb{R}_{>0}$ . Then,  $z^i \in \mathbb{R}_{>0}$  for each  $i \leq n$  and  $a_i \neq 0$ . Note that  $z^m \in \mathbb{R}_{>0}$  and  $z^k \in \mathbb{R}_{>0}$  imply  $z^{m-k} \in \mathbb{R}_{>0}$ . As a consequence,  $z^{\delta_f} \in \mathbb{R}_{>0}$  for  $\delta_f = \gcd\{i \mid a_i \neq 0\}$ . Since  $z \neq x_+$ , we have  $\delta_f > 1$ . Part 1 of the lemma is proved.

From the definition of  $\delta_f$ ,  $f$  is a polynomial of  $x^{\delta_f}$ :  $f(x) = \hat{f}(x) \circ (x^{\delta_f})$ . It is easy to see that  $\hat{f}(x) \in \Phi_0$ . Let  $\hat{f}(x) = b_k x^k + \dots + b_1 x + b_0$ . Then  $\gcd\{j \mid b_j \neq 0\} = 1$ . By the first part of this lemma, we know  $x_+^{\delta_f}$  is the only root of  $f$  whose absolute value is  $x_+^{\delta_f}$ . Since  $z^{\delta_f}$  and  $x_+^{\delta_f}$  are both the unique positive real roots of  $\hat{f}(x)$ , we have  $z^{\delta_f} = x_+^{\delta_f}$  and hence  $z$  is a simple root of  $f$ . Part 2 of the lemma is proved. Part 3 of the lemma comes from the fact  $z^{\delta_f} = x_+^{\delta_f}$  is the unique positive real root of  $f$  and  $f(z) = \hat{f}(z^{\delta_f}) = 0$ .

**Corollary 4.4.** *If  $f \in \Phi_1$  has at least one positive real root  $x_+$ , then  $x_+$  is the unique positive real root of  $f$ ,  $x_+$  is simple and for any root  $z$  of  $f$ ,  $x_+ \geq |z|$ . If  $f$  has a root  $z \neq x_+$  satisfying  $|z| = x_+$ , then  $z$  is simple, and  $z^{\delta} \in \mathbb{R}_{>0}$  for some  $\delta \in \mathbb{N}_{>1}$ , or equivalently, the argument of  $z$  satisfies  $\text{Arg}(z)/\pi \in \mathbb{Q}$ .*

**Example 4.5.**  $f = (x^2 - 5)(x^2 - 2x + 5) \notin \Phi_1$ , because the root  $z = 1 + 2\mathbf{i}$  satisfies  $|z| = \sqrt{5}$  but  $z^{\delta} \notin \mathbb{R}_{>0}$  for any  $\delta \in \mathbb{N}$ .

The following example shows that the multiplicity for a root  $z$  satisfying  $|z| < x_+$  could be any number.

**Example 4.6.** *For any  $n, k \in \mathbb{N}_{>1}$ ,  $(x+1)^n(x-k) \in \Phi_1$ . Let  $n = 1$ ,  $(x+1)(x-k) \in \Phi_0$ . Let  $f_1(x) = (x+1)^2$  and  $f_{n+1}(x) = f_n(x)(x^{2^{\lfloor \deg(f_n)/2 \rfloor + 1}} + 1)$  for  $n > 1$ . Then we have  $(x+1)^{n+1} \mid f_n(x)$ ,  $f_n(x) \in \mathbb{Z}^{>0}[x]$ , and all coefficients of  $f_n$  are either 1 or 2. Thus,  $f_n(x)(x-k) \in \Phi_0$  and  $(x+1)^n(x-k) \in \Phi_1$  by definition.*

**Lemma 4.7.** Let  $q(x) \in \mathbb{Z}[x]$  be a primitive irreducible polynomial and  $\delta \in \mathbb{N}_{>1}$ . Then  $(q)_{\mathbb{Z}[x]} \cap \mathbb{Z}[x^\delta] = (\tilde{q}(x^\delta))_{\mathbb{Z}[x^\delta]}$ , where  $\tilde{q} \in \mathbb{Z}[x]$  is primitive and irreducible and  $\tilde{q}(x^\delta)^m = R_u(u^\delta - x^\delta, q(u))$  for some  $m \in \mathbb{N}$ . We use  $R_u$  to denote the Sylvester resultant w.r.t. the variable  $u$ . Furthermore, the roots of  $\tilde{q}(x)$  are  $\{z^\delta \mid q(z) = 0\}$ .

*Proof:* Let  $q(x) = a \prod_{j=1}^n (x - z_j)$ ,  $\zeta_\delta = e^{2\pi i/\delta}$ , and

$$\bar{R}(x^\delta) = R_u(u^\delta - x^\delta, q(u)) = \prod_{l=1}^{\delta} q(\zeta_\delta^l x).$$

We claim that  $\bar{R}(x^\delta)$  is primitive. We have  $\text{lc}(R_u(u^\delta - x^\delta, q(u))) = \text{lc}(\prod_{l=1}^{\delta} q(\zeta_\delta^l x)) = a^\delta$ . Let  $c \in \mathbb{Z}$  be a prime factor of  $a^\delta$  or  $a$ . Since  $q$  is primitive,  $q \not\equiv 0 \pmod{c}$ . Let  $q(x) = bx^m + \dots \pmod{c}$ . Then  $\text{lt}(\bar{R}(x^\delta)) = \text{lt}(\prod_{l=1}^{\delta} q(\zeta_\delta^l x)) = \prod_{l=1}^{\delta} b(\zeta_\delta^l x)^m = b^\delta x^{\delta m} \not\equiv 0 \pmod{c}$ . So  $c \nmid \bar{R}(x^\delta)$  and thus  $\bar{R}(x^\delta)$  is primitive.

Since  $\mathbb{Q}[x^\delta]$  is a PID and  $\bar{R}(x^\delta) \in (q)_{\mathbb{Q}[x]} \cap \mathbb{Q}[x^\delta]$ , there exists a primitive polynomial  $\tilde{q} \in \mathbb{Z}[x]$  such that  $(\tilde{q}(x^\delta))_{\mathbb{Q}[x^\delta]} = (q)_{\mathbb{Q}[x]} \cap \mathbb{Q}[x^\delta]$ . Since  $q(x) \mid \tilde{q}(x^\delta)$  and  $q$  is irreducible,  $\tilde{q}(x)$  must be irreducible. Since both  $q(x)$  and  $\tilde{q}(x)$  are primitive, we can deduce  $(\tilde{q}(x^\delta))_{\mathbb{Z}[x^\delta]} = (q)_{\mathbb{Z}[x]} \cap \mathbb{Z}[x^\delta]$  from  $(\tilde{q}(x^\delta))_{\mathbb{Q}[x^\delta]} = (q)_{\mathbb{Q}[x]} \cap \mathbb{Q}[x^\delta]$ .

Since  $q(x) \mid \tilde{q}(x^\delta)$ ,  $Z_\delta = \{\zeta_\delta^k z_j \mid k = 1, \dots, \delta, j = 1, \dots, n\}$  is a subset of the roots of  $\tilde{q}(x^\delta)$ . Let  $\bar{S}(x)$  be the square-free part of  $\bar{R}(x) \in \mathbb{Z}[x]$ , which is also primitive. Since  $Z_\delta$  contains exactly the roots of  $\bar{R}(x^\delta)$  and  $\bar{S}(x^\delta)$ , we have  $\bar{S}(x) \mid \tilde{q}(x)$ . Since  $\tilde{q}(x)$  is irreducible and  $\bar{S}(x)$  is the square-free part of  $\bar{R}(x)$ , we have  $\bar{S}(x) = \tilde{q}(x)$  and hence  $\bar{R}(x^\delta) = \tilde{q}(x^\delta)^m$  for some  $m \in \mathbb{N}[x]$ . Finally, since the roots of  $\tilde{q}(x^\delta)$  are  $\mathbb{Z}_\delta$ , the roots of  $\tilde{q}(x)$  are  $\{z^\delta \mid q(z) = 0\}$ .

**Corollary 4.8.** Let  $\delta \in \mathbb{N}$  and  $f = \prod_{j=1}^m q_j^{\alpha_j}$ , where  $\alpha_j \in \mathbb{N}$  and  $q_j$  are primitive irreducible polynomials in  $\mathbb{Z}[x]$  with positive leading coefficients. Let  $q_i^*(x^\delta)$  be the square-free part of  $R_u(u^\delta - x^\delta, q_i(u))$  and  $f^* \triangleq \text{lcm}(\{q_j^{*\alpha_j} \mid j\})$ . Then

$$(f)_{\mathbb{Z}[x]} \cap \mathbb{Z}[x^\delta] = (f^*(x^\delta))_{\mathbb{Z}[x^\delta]}. \quad (14)$$

Furthermore, the roots of  $f^*(x)$  are  $\{z^\delta \mid f(z) = 0\}$ .

*Proof:* By Lemma 4.7, we have  $(q_i)_{\mathbb{Z}[x]} \cap \mathbb{Z}[x^\delta] = (q_i^*(x^\delta))_{\mathbb{Z}[x^\delta]}$ . Then  $(f)_{\mathbb{Z}[x]} \cap \mathbb{Z}[x^\delta] = \bigcap_{i=0}^s ((q_i^{\alpha_i})_{\mathbb{Z}[x]} \cap \mathbb{Z}[x^\delta]) = \bigcap_{i=0}^s (q_i^{*\alpha_i})_{\mathbb{Z}[x^\delta]} = (\text{lcm}(\{q_i^{*\alpha_i} \mid i\}))_{\mathbb{Z}[x^\delta]} = (f^*(x^\delta))_{\mathbb{Z}[x^\delta]}$ . From  $f^* \triangleq \text{lcm}(\{q_j^{*\alpha_j} \mid j\})$  and Lemma 4.7, the roots of  $f^*(x)$  are  $\{z^\delta \mid f(z) = 0\}$ .

**Theorem 4.9.** Let  $f \in \mathbb{Z}[x]$  have a unique positive root  $x_+$  and any root  $w$  of  $f$  satisfies  $|w| \leq x_+$ . If there exists a minimal  $\delta \in \mathbb{N}_{>1}$  such that for all root  $z \neq x_+$  of  $f$ ,  $|z| = x_+$  implies  $z^\delta \in \mathbb{R}_{>0}$ . Let  $f^*(x^\delta) \in \mathbb{Z}[x^\delta]$  be the polynomial in (14). Then  $f \in \Phi_1$  if and only if  $\text{lc}(f) = \text{lc}(f^*)$  and  $f^* \in \Phi_1$ .

*Proof:* “ $\Leftarrow$ ” Since  $\text{lc}(f) = \text{lc}(f^*)$  and  $(f) \cap \mathbb{Z}[x^\delta] = (f^*(x^\delta))$ , there exists a monic polynomial  $h \in \mathbb{Z}[x]$  such that  $f^*(x^\delta) = fh$ . Since  $f^* \in \Phi_1$ , there exists a monic polynomial  $g \in \mathbb{Z}[x]$  such that  $f^*(x)g(x) \in \Phi_0$ . Then  $f^*(x^\delta)g(x^\delta) = fhg(x^\delta) \in \Phi_0$ . Since  $hg(x^\delta)$  is monic, we have  $f \in \Phi_1$ .

“ $\Rightarrow$ ” Since  $f \in \Phi_1$ , there exists a primitive polynomial  $h \in (f) \cap \Phi_0$  with  $h(0) \neq 0$  and  $\text{lc}(h) = \text{lc}(f)$ . Each such  $h$  has some roots whose absolute value is  $x_+$ . Since  $f \mid h$ , by part 3 of Lemma 4.3 we have  $\delta \mid \delta_h$ , where  $\delta_h = \gcd\{k \mid x^k \text{ is in } h\}$ . By Lemma 4.3,  $h \in \mathbb{Z}[x^{\delta_h}] \subset \mathbb{Z}[x^\delta]$ . Thus  $h \in (f) \cap \mathbb{Z}[x^\delta] = (f^*)_{\mathbb{Z}[x^\delta]}$ . Since  $\text{lc}(f) \mid \text{lc}(f^*) \mid \text{lc}(h)$  and  $\text{lc}(f) = \text{lc}(h)$ , we have  $\text{lc}(f) = \text{lc}(f^*) = \text{lc}(h)$ , so  $f^* \in \Phi_1$ .

**Example 4.10.** Let  $f = (x^2 - 2)(x + 1)$ . Then  $\delta = 2$  and  $f^* = (x - 2)(x - 1)$  has two positive roots and hence  $f \notin \Phi_1$  by Corollary 4.4 and Theorem 4.9.

Let  $f_1 = x^2 - 2$ ,  $f_2 = x^2 - 2x + 2$ , and  $f = f_1 f_2$ . Then  $\delta = 8$ ,  $f_1^* = x - 16$ ,  $f_2^* = x - 16$ , and  $f^* = x - 16$ . Hence  $f \in \Phi_1$ .

**Corollary 4.11.** *Let  $f^*(x)$  be the polynomial defined in Theorem 4.9. Then  $f^*(x)$  has only one root (may be a multiple root) whose absolute value is  $x_+^\delta$  and any root  $z \neq x_+^\delta$  of  $f^*$  satisfies  $|z| < x_+^\delta$ .*

*Proof:* By Corollary 4.8, the roots of  $f^*(x)$  are  $\{z^\delta \mid f(z) = 0\}$ . Then the corollary comes from the fact that  $x_+$  is the unique positive real root of  $f$  and  $f(z) = 0, |z| = x_+$  imply  $z^\delta \in \mathbb{R}_{>0}$ .

By Corollary 4.11, when  $f$  has a unique positive real root  $x_+$ , we reduce the decision of  $f \in \Phi_1$  into the decision of  $f^* \in \Phi_1$ , where  $f^*$  has only one root with absolute value  $x_+^\delta$ .

**Lemma 4.12.** *If  $f \in \Phi_1 \setminus \Phi_0$  has a unique positive real root  $x_+$ , then  $x_+ \geq 1$ .*

*Proof:* There exists a monic polynomial  $g \in \mathbb{Z}[x]$  such that  $fg \in \Phi_0$ . Since  $f \notin \Phi_0$ ,  $g$  is not a monomial. Without loss of generality we assume  $g(0) \neq 0$ , and then  $\prod_{g(z)=0} |z| = |g(0)/\text{lc}(g)| = |g(0)| \geq 1$  which implies  $\max_{g(z)=0} (|z|) \geq 1$ . Since  $x_+$  is the unique positive root of  $fg$ , by Lemma 4.2, we have  $x_+ \geq \max_{g(z)=0} (|z|) \geq 1$ .

The following two lemmas give simple criteria to check whether  $f \in \Phi_1$  in the case of  $f(1) = 0$ .

**Lemma 4.13.** *Let  $f \in \mathbb{Z}[x]$  be a primitive polynomial,  $f(1) = 0$ . If  $\delta \in \mathbb{N}$  is the smallest number such that all root  $z$  of  $f$  satisfies  $z^\delta = 1$ , then  $f \in \Phi_1$  if and only if  $f^*(x) = x - 1$ , where  $f^*$  is defined in (14).*

*Proof:* By Theorem 4.9, if  $f^*(x) = x - 1$  then  $f \in \Phi_1$ . Suppose  $f \in \Phi_1$ . By Lemma 4.3, any root of  $f$  is simple and hence  $f$  is square-free. Let  $\delta = \text{lcm}\{m \in \mathbb{N} \mid z^m = 1\}$ . Since  $f$  is primitive,  $\delta \in \mathbb{N}$  is the smallest number such that  $f(x) \mid x^\delta - 1$  in  $\mathbb{Z}[x]$ . Therefore, so  $f^*(x) = x - 1$ .

**Example 4.14.** *Let  $f = (x - 1)(x^2 + 1)(x^3 + 1)$ . Then  $\delta = 12$  and  $f^* = x - 1$ . So,  $f \in \Phi_1$ . Let  $f = (x - 1)(x^2 + 1)^2(x^3 + 1)$ . Then  $\delta = 12$  and  $f^* = (x - 1)^2$ . So,  $f \notin \Phi_1$ .*

**Lemma 4.15.** *If  $f(1) = 0$  and any other root  $z$  of  $f$  satisfies  $|z| < 1$ , then  $f \in \Phi_1$  if and only if  $f(x)/(x - 1) \in \mathbb{Z}[x^\delta]$  for some  $\delta \in \mathbb{N}_{>0}$  and  $f(x)(x^\delta - 1)/(x - 1) \in \Phi_0$ .*

*Proof:* The necessity is obvious. For the other direction, there exists a monic polynomial  $g \in \mathbb{Z}[x]$  such that  $fg \in \Phi_0$ . We claim that each root  $z$  of  $g$  has absolute value 1. Since  $g$  is monic,  $\prod_{g(z)=0} |z| \geq 1$ . Since  $fg \in \Phi_0$  and  $f(1) = 0$ ,  $\max_{g(z)=0} |z| \leq 1$ , and the claim is proved.

By Lemma 4.2,  $fg \in \mathbb{Z}[x^\delta]$ , where  $\delta = \delta_{fg}$ . Since  $f(1) = 0$  and all other roots of  $f$  have absolute value  $< 1$ , we have  $(x^\delta - 1) \mid fg$  and  $((x^\delta - 1)/(x - 1)) \mid g$ . By part 3 of Lemma 4.3, the roots of  $fg$  with absolute value 1 are exactly the roots of  $x^\delta - 1$ . Since the absolute values of all roots of  $g$  is 1 and  $g$  has no multiple roots by Lemma 4.3,  $g = (x^\delta - 1)/(x - 1)$ . Since  $fg \in \mathbb{Z}[x^\delta]$  and  $(x^\delta - 1) \mid fg$ , set  $fg = (x^\delta - 1)h(x^\delta)$  for  $h \in \mathbb{Z}[x]$ . From  $g = (x^\delta - 1)/(x - 1)$ , we have  $f/(x - 1) = h(x^\delta) \in \mathbb{Z}[x^\delta]$ .

Now, only when  $f \notin \Phi_0$ ,  $f$  has a unique positive real root  $x_+ > 1$ , and any other root of  $f$  has absolute value  $< x_+$ , we do not know how to decide  $f \in \Phi_1$ . By computing many examples, we propose the following conjecture.

**Conjecture 4.16.** *If  $f \in \mathbb{Z}[x] \setminus \Phi_0$  has a simple and unique positive real root  $x_+$ ,  $x_+ > 1$ , and  $x_+ > |z|$  for any other root  $z$  of  $f$ , then  $f \in \Phi_1$ .*

## 4.2 Algorithm for $f \in \Phi_1$

Based on the results proved in the preceding section, we give the following algorithm to decide whether  $f \in \Phi_1$ . Note that the last step of the algorithm depends on whether Conjecture 4.16 is true.

---

**Algorithm 1 — Membership $\Phi_1(f)$** 


---

**Input:**  $f \in \mathbb{Z}[x]$  such that  $\text{lc}(f) > 0$ ,  $f(0) \neq 0$ , and  $f$  is primitive.

**Output:** Whether  $f \in \Phi_1$ .

1. If  $\text{lt}(f) = f^+$ , then  $f \in \Phi_0 \subset \Phi_1$ .
  2. If  $f$  has no positive real roots, then  $f \in \Phi_1$ .
  3. If  $f$  has at least two positive real roots (with multiplicities counted), then  $f \notin \Phi_1$ .
  4. Let  $x_+$  be the simple and unique positive real root of  $f$ .
    - 4.1. If  $x_+ < 1$ , or equivalently  $f(1) > 0$ , then  $f \notin \Phi_1$ .
    - 4.2. If  $x_+ = 1$  and all root  $z$  of  $f$  satisfies  $z^\delta = 1$  for some  $\delta \in \mathbb{N}$ , then  $f \in \Phi_1$  if and only if  $f^* = x - 1$ , where  $f^*$  is defined in (14).
    - 4.3. If  $x_+ = 1$  and any other root  $z$  of  $f$  satisfies  $|z| < 1$ , then  $f \in \Phi_1$  if and only if  $f(x)/(x-1) \in \mathbb{Z}[x^\delta]$  for some  $\delta \in \mathbb{N}_{>1}$  and  $f(x)(x^\delta - 1)/(x-1) \in \Phi_0$ .
    - 4.4. If  $f$  has a root  $z$  such that  $|z| > x_+$ , then  $f \notin \Phi_1$ .
    - 4.5. If  $f$  has a root  $z$  such that  $z \neq x_+$ ,  $|z| = x_+$ , and  $(\frac{z}{x_+})^\delta \neq 1$  for any  $\delta \in \mathbb{N}_{>1}$ , then  $f \notin \Phi_1$ .
    - 4.6. Let  $\delta$  be the minimal integer such that  $f(z) = 0$ ,  $z \neq x_+$ , and  $|z| = x_+$  imply  $(\frac{z}{x_+})^\delta = 1$ . Then  $f \in \Phi_1$  if and only if  $\text{lc}(f) = \text{lc}(f^*)$  and  $f^* \in \Phi_1$ , where  $f^*$  is defined in (14). If  $\text{lc}(f) = \text{lc}(f^*)$  then return **Membership $\Phi_1(f^*)$** , otherwise return false.
    - 4.7. If  $f$  does not satisfy all the above conditions, then it satisfies the condition of Conjecture 4.16 and  $f \in \Phi_1$  if the conjecture is valid.
- 

In what below, we will give the details for Algorithm 1 and prove its correctness. We will use algorithms for real root isolation and complex root isolation for univariate polynomials. Please refer to the latest work on these topics and references in these papers [2, 19].

Step 1 is trivial to check. Step 2 can be done with any real root isolation algorithm. Step 3 can be done by first factoring  $f$  as the product of irreducible polynomials and then isolating the real roots of each factor of  $f$ .

Step 4.1 is trivial to check. For Step 4.2, there exists a  $\delta \in \mathbb{N}$  such that  $(z)^\delta = 1$  if and only if each irreducible factor of  $f(x)$  is a cyclotomic polynomial, which can be checked with the Graeffe method in [3] and the  $\delta$  can also be founded. The polynomial  $f^*$  in Step 4.2 can be computed with Corollary 4.8.

In Step 4.3, the  $\delta$  can be found from the fact  $f(x)/(x-1) \in \mathbb{Z}[x^\delta]$ . If  $f(x)(x^\delta - 1)/(x-1) \in \Phi_0$  for some  $\delta$  satisfying  $f(x)/(x-1) \in \mathbb{Z}[x^\delta]$ , then return true; otherwise return false.

In Steps 4.4, 4.5, and 4.6, we need to check whether  $f$  has a root  $z \neq x_+$  such that  $|z| > x_+$ ,  $|z| = x_+$ , and  $z^m \in \mathbb{R}_{>0}$  for some  $m \in \mathbb{N}$ . To do that, we first give a lemma.

**Lemma 4.17.** *Let  $p(x) = a \prod_{i=1}^n (x - x_i) \in \mathbb{Z}[x]$ ,  $q(x) = b \prod_{j=1}^m (x - y_j) \in \mathbb{Z}[x]$ , and  $x_i y_j \neq 0$  for all  $i, j$ . Then the roots of  $R_u(p(u), q(ux))$  are  $\{y_j/x_i \mid i = 1, \dots, n, j = 1, \dots, m\}$  and the roots of  $R_u(u^n p(x/u), q(u))$  are  $\{x_i y_j \mid i = 1, \dots, n, j = 1, \dots, m\}$ .*

*Proof:* The lemma comes from  $R_u(p(u), q(ux)) = a^m b^n \prod_{i,j} (x - x_j/y_i)$  and  $R_u(u^n p(x/u), q(u)) = a_0^m b^n \prod_{i,j} (x - x_i x_j)$ , where  $a_0 = p(0)$ .

In the rest of this section, we assume

$$\begin{aligned} f &= f_0 \prod_{i=1}^t f_i^{e_i} \\ r_i(x) &= R_u(u^n f_i(x/u), f_i(u)) \end{aligned} \tag{15}$$

where  $f_i$  are primitive and irreducible polynomials with positive leading coefficients. Also assume that  $f(x)$  has a unique positive root  $x_+$  which is the root of  $f_0(x)$ .

By Lemma 4.17, the real roots of all  $r_i(x)$  include  $x_+^2$  and  $z\bar{z}$ , where  $z$  is a complex root of  $r_i(x)$ . Then the condition in Step 4.4 of the algorithm can be checked with the following result based on real root isolation.

**Corollary 4.18.**  *$f$  has a root  $z$  such that  $|z| > x_+$  if and only if some  $r_i(x)$  has a positive root larger than  $x_+^2$ .*

It is easy to check whether  $-x_+$  is a root of  $f_i$ : since  $f_i$  is irreducible,  $-x_+$  is a root of  $f_i$  if and only if  $f_i(-x) = \pm f_i(x)$ . If  $z$  is complex root of  $f_i$  such that  $|z| = x_+$ , then  $x_+^2, x_+^2 = z\bar{z}, x_+^2 = \bar{z}z$  are all roots of  $r_i$ . Then, we have the following result.

**Corollary 4.19.** *Let  $m_i$  be the multiplicity of  $x_+^2$  as a root of  $r_i$  and  $n_i$  the multiplicity of  $-x_+$  as a root of  $f_i$  (the multiplicity is set to be zero if  $x_+^2$  or  $-x_+$  is not a root). Then  $\#\{z \mid f_0(z) = 0, |z| = x_+, z \notin \mathbb{R}\} = m_0 - n_0 - 1$  and  $\#\{z \mid f_i(z) = 0, |z| = x_+, z \notin \mathbb{R}\} = m_i - n_i$  for  $i > 0$ .*

As usual, a representation of a complex root  $z$  is a pair  $(p, B)$  where  $p$  is an irreducible polynomial and  $B$  a box such that  $p(z) = 0$  and  $z$  is the only root of  $p$  in  $B$ . A box is represented by its lower-left and upper-right vertexes:  $([x_l, y_l], [x_t, x_t])$ . By the following lemma, we can find representations for all roots  $z$  of  $f$  satisfying  $|z| = x_+$ .

**Lemma 4.20.** *Suppose  $f_i$  has  $s$  roots  $z_1, \dots, z_s$  satisfying  $|z_j| = x_+$ . Then, we can find representations for  $z_j$ .*

*Proof:* Since  $f_i$  is irreducible,  $f_i$  is the minimal polynomial for  $z_i$ . Suppose  $I = (a, b)$  is an isolation interval for  $x_+$ . By algorithms of complex root isolation and real root isolation, we can simultaneously refine  $I$  and the isolation boxes of the roots of  $f_i$  such that the number of isolation boxes meet the region  $a < |x| < b$  will eventually becomes  $s$ . These  $s$  boxes are the isolation boxes for  $z_1, \dots, z_s$ , since  $f_i$  has exactly  $s$  roots satisfying  $|z| = x_+$ .

**Lemma 4.21.** *Let  $z$  be a root of  $f_k$  satisfying  $|z| = x_+$ . Then, we can find a representation for  $z/x_+$ .*

*Proof:* Let  $H(x) = R_u(f_0(u), f_k(ux)) \in \mathbb{Z}[x]$  and  $h_i(x), i = 1, \dots, s$  the irreducible factors of  $H$ . From Lemma 4.17,  $H(z/x_+) = 0$  and  $h_c(z/x_+) = 0$  for certain  $c$  and we will show how to find  $h_c$ . Isolate the roots of  $h_i, i = 1, \dots, s$  and refine the isolation box  $B = ([x_l, y_l], [x_t, x_t])$  of  $z$  and the isolation interval of  $x_+ = (l, r)$  simultaneously such that  $([x_l/r, y_l/r], [x_t/l, x_t/l])$  intersects only one of the isolation boxes of  $h_i, i = 1, \dots, s$ . This box  $B_1$  should be the isolation box for  $z/x_+$ . If  $B_1$  contains a root of  $f_c$ , then  $f_c$  is the minimal polynomial for  $z/x_+$ .

With the following lemma, we can check whether  $z^m \in \mathbb{R}_{>0}$  for some  $m$ .

**Lemma 4.22.** *Let  $z$  be a root of  $f_k$  satisfying  $|z| = x_+$  and  $q$  the minimal polynomial for  $z/x_+$ . Then we can decide whether there exists an  $m \in \mathbb{N}$  such that  $(z/x_+)^m = 1$ , and if such an  $m$  exists, we can compute the minimal  $m$ .*

*Proof:* There exists an  $m \in \mathbb{N}$  such that  $(z/x_+)^m = 1$  if and only if  $q(x)$  is a cyclotomic polynomial, which we can be tested by the Graeffe method in [3]. The method also gives the  $m$  such that  $(z/x_+)^m = 1$ . The minimal  $m$  can be found easily.

Now, we consider Step 4.5. With Corollary 4.19 and Lemma 4.20, we can find all the roots  $z$  of  $f$  satisfying  $|z| = x_+$ . For each such  $z$ , we can check whether there exists a  $\delta_z \in \mathbb{N}$  such that  $(z/x_+)^{\delta_z} = 1$  with Lemma 4.22. Hence the conditions of Step 4.5 can be checked.

Now, we consider Step 4.6. The  $\delta$  in Step 4.6 can be computed as  $\delta = \text{lcm}\{\delta_z \mid f(z) = 0, |z| = x_+, (z/x_+)^{\delta_z} = 1\}$ . With  $\delta$  given,  $f^*$  in Step 4.6 can be computed with Corollary 4.8. From Corollary 4.8, the roots of  $f^*$  are  $\{z^\delta \mid f(z) = 0\}$ . As a consequence, when running **Membership** $\Phi_1(f^*)$ , only Steps 1, 3, 4.7 will be executed, and no further calls to **Membership** $\Phi_1(f^*)$  are needed.

### 4.3 Compute the finite $\sigma$ -Gröbner basis

Let  $f \in \Phi_1$ , we will show how to compute the finite  $\sigma$ -Gröbner basis for  $\mathcal{J}_f = \text{sat}(\mathbb{P}_f)$  in (6).

**Lemma 4.23.** *Let  $f \in \Phi_1$ ,  $h = fg \in \Phi_0$  for a monic  $g \in \mathbb{Z}[x]$ , and  $D = \deg(h)$ . Then*

$$\mathcal{J}_D = \text{sat}(\mathbb{P}_f) \cap \mathcal{F}[y, y^x, \dots, y^{x^D}] = \text{asat}(\mathbb{P}_f, \mathbb{P}_{xf}, \dots, \mathbb{P}_{x^{D-\deg(f)}f}) \quad (16)$$

and a Gröbner basis of  $\mathcal{J}_D$  is a  $\sigma$ -Gröbner basis of  $\mathcal{J}_f$ .

*Proof:* By the remark before Theorem 2.6,  $\mathbb{P}_f$  is regular and coherent. Then  $P \in \mathcal{J}_D$  if and only if  $\text{prem}(P, \mathbb{P}_f) = 0$  which is equivalent to  $P \in \text{asat}(\mathbb{P}_f, \mathbb{P}_{xf}, \dots, \mathbb{P}_{x^{D-\deg(f)}f})$  [7], and (16) is proved. By Corollary 3.4, a Gröbner basis of  $\mathcal{J}_D$  is a  $\sigma$ -Gröbner basis of  $\mathcal{J}_f$ .

The Gröbner basis of  $\mathcal{J}_D$ , denoted as  $\mathbb{G}(f, D)$ , can be computed with the following well-known fact

$$\text{asat}(\mathbb{P}_f, \mathbb{P}_{xf}, \dots, \mathbb{P}_{x^{D-\deg(f)}f}) = (z \cdot J^{\sum_{i=0}^{D-\deg(f)} x^i} - 1, \mathbb{P}_f, \mathbb{P}_{xf}, \dots, \mathbb{P}_{x^{D-\deg(f)}f}) \cap \mathcal{F}[y, y^x, \dots, y^{x^D}],$$

where  $J = \text{init}(\mathbb{P}_f)$  and  $z$  is a new indeterminate. Therefore, in order to compute the  $\sigma$ -Gröbner basis of  $\mathcal{J}_f$ , it suffices to compute  $D$ . We thus have the following algorithm.

---

#### Algorithm 2 — FiniteGB ( $f$ )

---

**Input:**  $f \in \Phi_1$  such that  $\text{lc}(f) > 0$ .

**Output:** Return  $\sigma$ -Gröbner basis of  $\mathcal{J}_f = \text{sat}(\mathbb{P}_f)$ .

1. If  $\text{lt}(f) = f^+$ , then return  $\{\mathbb{P}_f\}$ .
  2. If  $f$  has no positive real roots, then return  $\mathbb{G}(f, N_f + \deg(f) + 1)$ , where  $N_f$  is defined in Lemma 3.14.
  3. Let  $x_+$  be the unique simple positive real root of  $f$ .
    - 3.1. If  $x_+ = 1$  and all root  $z$  of  $f$  satisfies  $z^\delta = 1$  for some  $\delta \in \mathbb{N}$ , then return  $\mathbb{G}(f, \delta)$ .
    - 3.2. If  $x_+ = 1$  and any other root  $z$  of  $f$  satisfies  $|z| < 1$ , then return  $\mathbb{G}(f, \deg(f) + \delta - 1)$ , where  $\delta$  is found in Step 4.3 of Algorithm 1.
    - 3.3. Let  $\delta$  be the minimal integer such that  $f(z) = 0$ ,  $z \neq x_+$ , and  $|z| = x_+$  imply  $(\frac{z}{x_+})^\delta = 1$ . Let the  $f^*$  be defined (14) and  $f^*(x^\delta) = f(x)s(x)$ . Return  $\mathbb{G}(f, \delta \deg(f^*))$ .
- 

In the rest of this section, we will prove the correctness of the algorithm. Step 1 follows Lemma 3.2.

For Step 2, by Lemma 3.14,  $(x+1)^{N_f}f \in \mathbb{Z}^{>0}[x]$ . Following the proof of Lemma 3.6, for a sufficiently large  $M \in \mathbb{N}$ ,  $(x-M)(x+1)^{N_f}f \in \Phi_0$ . Then,  $D = \deg((x-M)(x+1)^{N_f}f) = N_f + \deg(f) + 1$ .

For Step 3.1, following Step 4.2 of Algorithm 1, we have  $f^*(x^\delta) = f(x)g(x) = x^\delta - 1$  for some  $g$ . Then  $D = \delta$ . For Step 3.2, following Step 4.3 of Algorithm 1,  $f(x)(x^\delta - 1)/(x - 1) \in \Phi_0$ . Then  $D = \deg(f) + \delta - 1$ .

For Step 3.3, from the proof of Step 4.6 of Algorithm 1, there exist three possibilities:  $f^*(x) \in \Phi_0$ ,  $f^*(x)$  has at least two positive roots, or  $f^*$  satisfies the conditions of Conjecture 4.16. Since we already assumed  $f^* \in \Phi_1$ , only  $f^*(x) \in \Phi_0$  is possible. From  $f^*(x^\delta) = f(x)s(x)$ , we have  $D = \delta \deg(f)$ . We now proved the correctness of Algorithm 2.

## 5 Approach based on integer programming and lower bound

Given an  $f \in \mathbb{Z}[x]$ , the existence of a monic polynomial  $g \in \mathbb{Z}[x]$  with  $\deg(g) \leq m$ , such that  $fg \in \Phi_0$  can be reduced to an integer programming problem. Based on this idea, a lower bound for  $\deg(g)$  is given in certain cases.

**Lemma 5.1.** *Given a polynomial  $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$  with  $a_n > 0$ , there exists a monic polynomial  $g \in \mathbb{Z}[x]$  with  $\deg(g) \leq m$ , such that  $fg \in \Phi_0$  if and only if a  $(b_{m-1}, \dots, b_0) \in \mathbb{Z}^m$  satisfies*

$$\begin{pmatrix} a_{n-1} & a_n & & & \\ \vdots & \vdots & \ddots & & \\ a_0 & a_1 & \cdots & a_n & \\ & \ddots & \ddots & \ddots & \ddots \\ & & a_0 & a_1 & \cdots & a_n \\ & & & \ddots & \ddots & \vdots \\ & & & & a_0 & a_1 \\ & & & & & a_0 \end{pmatrix}_{(m+n) \times (m+1)} \begin{pmatrix} 1 \\ b_{m-1} \\ b_{m-2} \\ \vdots \\ b_0 \end{pmatrix} \leq 0. \quad (17)$$

Moreover such  $g$  has degree  $< m$  if and only if  $b_0 = 0$  for some feasible solution of the above inequalities.

*Proof:* Let  $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$ . The leading coefficient of  $fg$  is  $a_n > 0$ , and the coefficient of  $x^k$  is the  $m+n-k$ -row of the left side of (17) for  $k = m+n-1, \dots, 0$ . If  $\deg(g) < m$ , the coefficients of  $g_1(x) = x^{m-\deg(g)}g(x)$  is a feasible solution with  $b_0 = 0$ . If  $b_0 = 0$ ,  $(1, b_{m-1}, \dots, b_1)$  is a feasible solution of (17) for  $m = m-1$ .

The following result gives another criterion for the existence of  $g$ .

**Lemma 5.2.** *Given a polynomial  $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$  with  $a_n > 0$ , let  $(1/f)(x) \triangleq \lambda_0 + \cdots + \lambda_m x^m + \cdots \in \mathbb{Z}[a_0^{-1}][[x]]$ . There exists a monic polynomial  $g \in \mathbb{Z}[x]$  with  $\deg(g) \leq m$  and  $fg \in \Phi_0$  if and only if there exists a  $(c_{m+n-1}, \dots, c_0) \in \mathbb{N}^{m+n}$  such that*

$$\begin{pmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \cdots & \lambda_{m+n-2} & \lambda_{m+n-1} \\ & \lambda_0 & \lambda_1 & \ddots & \ddots & \lambda_{m+n-2} \\ & & \ddots & \ddots & \ddots & \vdots \\ & & & \lambda_0 & \cdots & \lambda_m \end{pmatrix} \begin{pmatrix} c_{m+n-1} \\ c_{m+n-2} \\ \vdots \\ c_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix}. \quad (18)$$

*Proof:* Extending the proof of Lemma 5.1, let  $\mathbf{b}_{m+n-1} \triangleq (b_{m+n-1}, \dots, b_0)^T$ . For the following special Jordan form

$$J_j \triangleq \begin{pmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & 0 \end{pmatrix}_{j \times j}, \text{ we have } f(J_j) = \begin{pmatrix} a_0 & \cdots & a_n & & \\ & a_0 & \ddots & \ddots & \\ & & \ddots & \ddots & a_n \\ & & & a_0 & \vdots \\ & & & & a_0 \end{pmatrix}_{j \times j}.$$

By Lemma 5.1,  $fg \in \Phi_0$  if and only if  $f(J_{m+n})\mathbf{b} \in \mathbb{Z}_{\leq 0}^{m+n}$  for some  $(b_{m-1}, \dots, b_0) \in \mathbb{Z}^m$  with  $(b_{m+n-1}, \dots, b_m) = (0, \dots, 0, 1)$ . Let  $\mathbf{c} = (c_{m+n-1}, \dots, c_0)^T \triangleq -f(J_{m+n})\mathbf{b} \in \mathbb{N}^{m+n}$ . Then we have  $f(J_{m+n})^{-1}\mathbf{c} = (1/f)(J_{m+n})\mathbf{c} =$



−**b**, that is

$$\begin{pmatrix} \lambda_0 & \lambda_1 & \cdots & \lambda_{m+n-1} \\ & \lambda_0 & \ddots & \vdots \\ & & \ddots & \lambda_1 \\ & & & \lambda_0 \end{pmatrix} \begin{pmatrix} c_{m+n-1} \\ c_{m+n-2} \\ \vdots \\ c_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -1 \\ -b_{m-1} \\ \vdots \\ -b_0 \end{pmatrix}.$$

Since we need only to know the existence of  $c_i$ , only the first  $n$  rows are need, and the lemma is proved.

Note that  $a_0^{i+1} \lambda_i \in \mathbb{Z}$  for any  $i \in \mathbb{N}$ . We can reduce the coefficient matrix in the above lemma into an integer matrix.

**Corollary 5.3.** *Let  $f, g \in \mathbb{R}[x]$ ,  $\text{lc}(f) > 0$ ,  $g$  monic, and  $(1/f)(x) \triangleq \sum_{m=0}^{\infty} \lambda_m x^m \in \mathbb{R}[[x]]$ . If  $\text{lt}(fg) = (fg)^+$ , then  $\deg(g) \geq \min\{j \in \mathbb{N} \mid \lambda_j < 0\}$ .*

*Proof:* From the proof of Lemma 5.2, there exists a monic  $g \in \mathbb{R}[x]$  such that  $\text{lt}(fg) = (fg)^+$  if and only if (18) has a solution  $(c_{m+n-1}, \dots, c_0) \in \mathbb{R}_{>0}^{m+n}$ . If  $\lambda_0, \dots, \lambda_m \geq 0$ , the last coordinate of (18) is  $\sum_{j=0}^m \lambda_j c_{m-j} \geq 0$ , hence  $\sum_{j=0}^m \lambda_j c_{m-j} \neq -1$  and (18) has no solution in  $\mathbb{R}_{>0}^{m+n}$ . As a consequence, if  $\text{lt}(fg) = (fg)^+$ , then  $\deg(g) \geq \min\{j \in \mathbb{N} \mid \lambda_j < 0\}$  and the corollary is proved.

**Corollary 5.4.** *Let  $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ ,  $a > 0$ ,  $b^2 - 4ac < 0$ , and  $z$  a root of  $f$ . If  $fg \in \Phi_0$  and  $g$  is monic, then  $\deg(g) \geq \lfloor \pi/|\text{Arg}(z)| \rfloor = \lfloor \pi/\arctan(\sqrt{4ac - b^2}/b) \rfloor$ .*

*Proof:* Let  $f(x) = a(x-z)(x-\bar{z})$ , and  $z = re^{\theta i}$  where  $r \in \mathbb{R}_{>0}$  and  $\theta = \text{Arg}(z) \neq k\pi$ . Without loss of generality, we can assume  $0 < \theta < \pi$ . Then

$$\frac{1}{f(x)} = \frac{1}{a(x-z)(x-\bar{z})} = \sum_{j=0}^{\infty} \frac{z^{j+1} - \bar{z}^{j+1}}{a(z\bar{z})^{j+1}(z-\bar{z})} x^j = \sum_{j=0}^{\infty} \frac{\sin((j+1)\theta)}{ar^{j+2} \sin \theta} x^j,$$

that is,  $\lambda_j = \frac{\sin((j+1)\theta)}{ar^{j+2} \sin \theta}$ . Since  $\lambda_0 = \frac{1}{ar^2} > 0$ ,  $\min\{j \in \mathbb{N} \mid \lambda_j < 0\} = \min\{j \in \mathbb{N} \mid (j+1)\theta > \pi\} = \lfloor \pi/\theta - 1 \rfloor + 1 = \lfloor \pi/\theta \rfloor$ . By Corollary 5.3,  $\deg(g) \geq \lfloor \pi/\theta \rfloor = \lfloor \pi/\arctan(\sqrt{4ac - b^2}/b) \rfloor$ .

We can now give a lower bound for the degree of  $g$  such that  $fg \in \Phi_0$  in certain case.

**Theorem 5.5.** *If a polynomial  $f(x) \in \mathbb{Z}[x]$  is of degree  $n$  and has at least one root not in  $\mathbb{R}$ , then  $\min\{\deg(g) \mid g \in \mathbb{Z}[x] \text{ is monic and } fg \in \Phi_0\} \geq \max\{\lfloor \pi/|\text{Arg}(z)| \rfloor - n + 2 \mid f(z) = 0, z \notin \mathbb{R}\}$ .*

*Proof:* Since  $f(x) \in \mathbb{Z}[x]$  has at least one root not in  $\mathbb{R}$ ,  $f = f_1 f_2$  where  $f_2$  is a quadratic polynomial in  $\mathbb{R}[x]$  which has two complex roots. Suppose there exists a monic  $g \in \mathbb{R}[x]$  such that  $\text{lt}(fg) = (fg)^+$  or  $\text{lt}(f_1 f_2 g) = (f_1 f_2 g)^+$ . By Corollary 5.4,  $\deg(g) \geq \lfloor \pi/|\text{Arg}(z)| \rfloor - \deg(f_1) = \lfloor \pi/|\text{Arg}(z)| \rfloor - n + 2$ . Then,  $\min\{\deg(g) \mid g \in \mathbb{Z}[x] \text{ is monic and } fg \in \Phi_0\} \geq \min\{\deg(g) \mid g \in \mathbb{R}[x] \text{ is monic and } \text{lt}(fg) = (fg)^+\} \geq \max\{\lfloor \pi/|\text{Arg}(z)| \rfloor - n + 2 \mid f(z) = 0, z \notin \mathbb{R}\}$ .

The following result shows that the lower bound given in the preceding theorem is also the upper bound for quadratic polynomials.

**Proposition 5.6.** *Let  $f(x) = a_2 x^2 + a_1 x + a_0 = a_2(x-z)(x-\bar{z})$  be a quadratic polynomial in  $\mathbb{Z}[x]$  with a root complex  $z = a + bi = re^{\theta i}$ , where  $a_2, b, r > 0$ ,  $0 < \theta < \pi$ ,  $\bar{z} = a - bi$ . Then  $\min\{\deg(g) \mid g \in \mathbb{Z}[x] \text{ and monic, } fg \in \Phi_0\} = \lfloor \pi/\theta \rfloor$ .*

*Proof:* If  $\pi/2 < \theta < \pi$ , then  $a_1 = -2a > 0$  and hence  $f \in \mathbb{N}^{>0}[x]$ . By the proof of Lemma 3.6, there exists an  $N$  such that  $(x - N)f \in \Phi_0$  and hence  $\widehat{\deg}(f) = 1 = \lfloor \pi/\theta \rfloor$ . If  $\theta = \pi/2$ , then  $f = a_2x^2 + a_0$ . It is easy to check  $\widehat{\deg}(f) = 2 = \lfloor \pi/\theta \rfloor$ .

From now on, we assume  $0 < \theta < \pi/2$ , so  $a > 0$  and  $a_1 < 0$ . Considering  $f_1(x) = (x - a - bi)(x - a + bi) = x^2 - 2ax + a^2 + b^2 \in \mathbb{Z}[a_2^{-1}][x]$ , we will solve the integer programming mentioned in Lemma 5.1:

$$\begin{pmatrix} -2a & 1 & & & \\ a^2 + b^2 & -2a & 1 & & \\ & \ddots & \ddots & \ddots & \\ & & a^2 + b^2 & -2a & 1 \\ & & & a^2 + b^2 & -2a \\ & & & & a^2 + b^2 \end{pmatrix}_{(m+2) \times (m+1)} \begin{pmatrix} 1 \\ b_{m-1} \\ b_{m-2} \\ \vdots \\ b_0 \end{pmatrix} \leq 0. \quad (19)$$

Let  $\Delta_1 = -2a$  and  $\Delta_{j+1} = -2a - (a^2 + b^2)/\Delta_j$  for  $j > 1$ . Then

$$\Delta_j = -\frac{(a + bi)^{j+1} - (a - bi)^{j+1}}{(a + bi)^j - (a - bi)^j} = -\frac{r \sin(j+1)\theta}{\sin j\theta}.$$

Let  $m_0 = \lceil \pi/\theta \rceil - 1$ . Then we have  $\Delta_j < 0$  for  $j = 1, \dots, m_0 - 1$  but  $\Delta_{m_0} \geq 0$ .

We will do row transformations on (19) to relax its feasible region. Let  $m = m_0 - 1$ . We add  $(m+1)$ -th row multiplied by  $1/(-\Delta_1) > 0$  to the  $m$ -th row. Then the  $-2a$  at the  $m$ -th row becomes  $\Delta_2 = -2a - (a^2 + b^2)/\Delta_1$ , and the 1 at the  $m$ -th row becomes 0. Then add  $m$ -th row multiplied by  $1/(-\Delta_2) > 0$  to the  $(m-1)$ -th row. Repeat the above process until  $\Delta_{m_0} \geq 0$ , and we obtain a lower triangular matrix:

$$\begin{pmatrix} \Delta_{m_0} & 0 & & & \\ a^2 + b^2 & \Delta_{m_0-1} & 0 & & \\ & \ddots & \ddots & \ddots & \\ & & a^2 + b^2 & \Delta_2 & 0 \\ & & & a^2 + b^2 & \Delta_1 \\ & & & & a^2 + b^2 \end{pmatrix}_{m_0+1 \times m_0}. \quad (20)$$

1. If  $\Delta_{m_0} > 0$ , the first coordinate of the left side of

$$\begin{pmatrix} \Delta_{m_0} & & & & \\ a^2 + b^2 & \Delta_{m_0-1} & & & \\ & \ddots & \ddots & \ddots & \\ & & a^2 + b^2 & \Delta_1 & \\ & & & a^2 + b^2 & \end{pmatrix} \begin{pmatrix} 1 \\ b_{m_0-2} \\ b_{m_0-3} \\ \vdots \\ b_0 \end{pmatrix} \leq 0 \quad (21)$$

is  $\Delta_{m_0} > 0$ . So the feasible region of (21) is empty and hence the feasible region of (19) is also empty. Thus  $fg \notin \Phi_0$  for any monic polynomial  $g$  of degree  $< m_0$  by Lemma 5.1.

Let  $m = m_0$ . We have

$$\begin{pmatrix} -2a & 1 & & & \\ a^2 + b^2 & \Delta_{m_0} & & & \\ & a^2 + b^2 & \Delta_{m_0-1} & & \\ & & \ddots & \ddots & \\ & & & a^2 + b^2 & \Delta_1 \\ & & & & a^2 + b^2 \end{pmatrix} \begin{pmatrix} 1 \\ b_{m_0-1} \\ b_{m_0-2} \\ \vdots \\ b_0 \end{pmatrix} \leq 0. \quad (22)$$

Similarly, we can obtain a quasi-upper triangular matrix from (19) by row transformations:

$$\begin{pmatrix} \Delta_1 & 1 & & & \\ & \ddots & \ddots & & \\ & & \Delta_{m_0-1} & 1 & \\ & & & \Delta_{m_0} & 1 \\ & & & a^2 + b^2 & -2a \end{pmatrix} \begin{pmatrix} 1 \\ b_{m_0-1} \\ b_{m_0-2} \\ \vdots \\ b_0 \end{pmatrix} \leq 0. \quad (23)$$

Combining (19), (22) and (23), we have

$$b_{m_0-1} \leq -\frac{a^2 + b^2}{\Delta_{m_0}} \Rightarrow b_{m_0-1} < 0 \Rightarrow -2a + b_{m_0-1} \leq 0; \quad (24)$$

$$-\frac{a^2 + b^2}{\Delta_{j+1}} b_{j+1} \leq b_j \leq -(a^2 + b^2) b_{j+2} + 2ab_{j+1}, \quad j = m_0 - 2, m_0 - 3, \dots, 0; \quad (25)$$

$$b_j \leq -(a^2 + b^2) b_{j+2} + 2ab_{j+1} \Rightarrow b_j \leq -\Delta_{m_0-j} b_{j+1} \Rightarrow b_j < 0, \quad j = m_0 - 2, m_0 - 3, \dots, 1; \quad (26)$$

$$b_0 \leq 0 \Rightarrow \Delta_{m_0} b_1 + b_0 \leq 0. \quad (27)$$

In (25), we need to show that there exists a rational number  $b_j$  satisfying

$$-\frac{a^2 + b^2}{\Delta_{j+1}} b_{j+1} < b_j < -(a^2 + b^2) b_{j+2} + 2ab_{j+1}. \quad (28)$$

We need to show

$$-(a^2 + b^2) b_{j+2} + 2ab_{j+1} + \frac{a^2 + b^2}{\Delta_{j+1}} b_{j+1} = -(a^2 + b^2) b_{j+2} - \Delta_{j+2} b_{j+1} > 0,$$

which is true from the first ' $<$ ' in (28) when  $j = j + 1$ .

Then we can choose some rational number  $b_{m_0-1}, \dots, b_0$  satisfying (24) and (28), and then  $(1, b_{m_0-1}, \dots, b_0)$  is a feasible solution of (19). Taking the common denominator  $N \in \mathbb{N}_{\geq 1}$  of  $\{b_j \mid j = 0, \dots, m_0 - 1\}$ , we have

$$\begin{aligned} -2a + Nb_{m_0-1} &< -2a + b_{m_0-1} \leq 0; \\ a^2 + b^2 - 2aNb_{m_0-1} + Nb_{m_0-2} &< N(a^2 + b^2 - 2ab_{m_0-1} + b_{m_0-2}) \leq 0; \\ (a^2 + b^2)Nb_j - 2aNb_{j-1} + Nb_{j-2} &\leq 0, \quad j = m_0 - 1, \dots, 2; \\ (a^2 + b^2)Nb_1 - 2aNb_0 &\leq 0; \quad (a^2 + b^2)Nb_0 \leq 0, \end{aligned}$$

and then

$$f(x)g_1(x) = a_2(x^2 - 2ax + a^2 + b^2)(x^{m_0} + \sum_{j=0}^{m_0-1} Nb_j x^j) \in \Phi_0. \quad (29)$$

Then  $\Delta_{m_0} > 0$  implies  $\widehat{\deg}(f) = m_0 = \lceil \pi/\theta \rceil - 1 = \lfloor \pi/\theta \rfloor$ .

2. If  $\Delta_{m_0} = 0$ ,  $\pi/\theta = m_0 + 1 > 2$ ,  $z = re^{\pi i/(m_0+1)}$ . Then  $e^{2\pi i/(m_0+1)}$  is a root of  $(x-1)^{-2}R_u(f(x), f(ux)) = a_2a_0x^2 + (2a_2a_0 - a_1^2)x + a_2a_0$ . Since  $e^{2\pi i/(m_0+1)}$  is integral over  $\mathbb{Z}$ , we have  $a_0a_2 \mid (2a_2a_0 - a_1^2)$  or  $a_0a_2 \mid a_1^2$ . For  $0 < 2\pi/(m_0+1) < \pi$ ,  $a_2a_0x^2 + (2a_2a_0 - a_1^2)x + a_2a_0$  has no real roots, and then we have  $(2a_2a_0 - a_1^2)^2 - 4(a_2a_0)^2 < 0$ , that is  $a_1^2 < 4a_0a_2$ . Then we have  $m_0 = 2$  when  $a_1^2 = a_0a_2$ ,  $m_0 = 3$  when  $a_1^2 = 2a_0a_2$  or  $m_0 = 5$  when  $a_1^2 = 3a_0a_2$ .

- (a) If  $m_0 = 2$  and  $\Delta_2 = 0$ ,  $f(x) = a_2x^2 + a_1x + a_0$ , where  $a_1 = -\sqrt{a_0a_2}$ . When solving (19) for  $m = 3$ , we have

$$b_0 \leq \frac{a_0^3}{a_1^3}, \quad b_1 \leq -\frac{a_1b_0}{a_0}, \quad -\frac{a_0^2 + a_1^2b_1}{a_0a_1} \leq b_2 \leq -\frac{a_1^2b_0 + a_0a_1b_1}{a_0^2}.$$

In order for an integer  $b_2$  to satisfy these inequations, we need to assume

$$\frac{a_1^2b_0 - a_0a_1b_1}{a_0^2} + \frac{a_0^2 + a_1^2b_1}{a_0a_1} \geq 2, \quad \text{that is } b_0 \leq \frac{a_0^3 - 2a_0^2a_1}{a_1^3}.$$

Here  $b_0 < 0$  implies  $\min\{\deg(g) \mid fg \in \Phi_0\} \geq 3$ , so  $\widehat{\deg}(f) = 3 = \pi/\theta = \lfloor \pi/\theta \rfloor$ .

- (b) If  $m_0 = 3$  and  $\Delta_3 = 0$ ,  $f(x) = a_2x^2 + a_1x + a_0$ , where  $a_1 = -\sqrt{2a_0a_2}$ . When we solve (19) for  $m = 4$ , we have

$$b_0 \leq \frac{-a_0^2}{a_2^2}, \quad b_3 \leq \frac{a_0^2a_1 + a_1a_2^2b_0}{-a_0^2a_2},$$

$$\frac{-a_2^2b_0 + a_0a_1b_3}{-a_0a_2} \leq b_2 \leq \frac{-a_0 - a_1b_3}{a_2}, \quad \frac{-a_2b_0 - a_0b_2}{a_1} \leq b_1 \leq \frac{-a_1b_2 - a_0b_3}{a_2}.$$

When we want

$$\frac{-a_1b_2 - a_0b_3}{a_2} - \frac{-a_2b_0 - a_0b_2}{a_1} \geq 2, \quad \frac{-a_0 - a_1b_3}{a_2} - \frac{-a_2^2b_0 + a_0a_1b_3}{-a_0a_2} \geq 2,$$

we only need

$$b_0 \leq \min\left\{\frac{-a_0^2 + 2a_1a_2}{a_2^2}, \frac{-a_0^2 - 2a_0a_2}{a_2^2}\right\}, \quad b_3 \leq \frac{a_0^2a_1 + a_1a_2^2b_0}{-a_0^2a_2}.$$

Here  $b_0 \leq -a_0^2/a_2^2 < 0$  implies  $\min\{\deg(g) \mid fg \in \Phi_0\} \geq 4$ , so  $\widehat{\deg}(f) = 4 = \pi/\theta = \lfloor \pi/\theta \rfloor$ .

- (c) If  $m_0 = 5$  and  $\Delta_5 = 0$ ,  $f(x) = a_2x^2 + a_1x + a_0$ , where  $a_1 = -\sqrt{3a_0a_2}$ . Rewriting  $a_2f(x) = a_2^2x^2 + a_2a_1x + 3a_1^2$ , When we solve (19) for  $a_2f(x)$  for  $m = 6$ , we get

$$b_5 < 0, \quad b_4 \leq \frac{-a_1^2 + 3a_1a_2b_5}{3a_2^2}, \quad \frac{a_1b_4}{a_2} \leq b_3 \leq \frac{3a_1a_2b_4 - a_1^2b_5}{3a_2^2}$$

$$\frac{2a_1b_3}{3a_2} \leq b_2 \leq \frac{3a_1a_2b_3 - a_1^2b_4}{3a_2^2}, \quad \frac{a_1b_2}{2a_2} \leq b_1 \leq \frac{3a_1a_2b_2 - a_1^2b_3}{3a_2^2}, \quad \frac{a_1b_1}{3a_2} \leq b_0 \leq \frac{3a_1a_2b_1 - a_1^2b_2}{3a_2^2}.$$

Because  $b_5 < 0$  implies  $\frac{a_1b_4}{a_2} < \frac{3a_1a_2b_4 - a_1^2b_5}{3a_2^2}$ ,  $\frac{a_1b_4}{a_2} < b_3$  implies  $\frac{2a_1b_3}{3a_2} < \frac{3a_1a_2b_3 - a_1^2b_4}{3a_2^2}$ ,  $\frac{2a_1b_3}{3a_2} < b_2$  implies  $\frac{a_1b_2}{2a_2} < \frac{3a_1a_2b_2 - a_1^2b_3}{3a_2^2}$ , and  $\frac{a_1b_2}{2a_2} < b_1$  implies  $\frac{a_1b_1}{3a_2} < \frac{3a_1a_2b_1 - a_1^2b_2}{3a_2^2}$ , there exists a feasible solution  $\{b_5, b_4, b_3, b_2, b_1, b_0\} \in \mathbb{Q}_{<0}^6$ , which is an inner point of the semi-algebraic set. Using the same notations in (29), let  $N \in \mathbb{N}_{>1}$  be the common denominator of  $\{b_0, \dots, b_5\}$ , and we have  $f(x)(x^6 + N \sum_{j=0}^5 b_j x^j) \in \Phi_0$ .

Here  $b_0 < 0$  implies  $\min\{\deg(g) \mid fg \in \Phi_0\} \geq 6$ , so  $\widehat{\deg}(f) = 6 = \pi/\theta = \lfloor \pi/\theta \rfloor$ .

We complete the proof.

The following example is used to illustrate the proof.

**Example 5.7.** Let  $f = x^2 - x + 2$ ,  $\Delta_1 = -1$ ,  $\Delta_2 = 1 > 0$ ,  $m_0 = 2$ ,  $\widehat{\deg}(f) = 2$ . Here  $f \notin \mathbb{N}[x]$  implies  $\widehat{\deg}(f) > 1$ , and  $(x^2 - x + 2)(x^2 - 5x - 7) \in \Phi_0$  implies  $\widehat{\deg}(f) \leq 2$ .

**Example 5.8.** Let  $f = x^2 - 2x + 2$ . By the effective Polya Theorem 3.14, we have  $d_1 = \min\{\deg(g) \mid g \in \mathbb{Z}[x] \text{ and monic, } fg \in \Phi_0\} \leq 10$ . However, we have  $\min\{\deg(g) \mid g \in \mathbb{Z}[x] \text{ and monic, } fg \in \Phi_0\} = 4$  by proposition 5.6, where  $g = x^4 - 2x^2 - 4x - 4$  and  $fg = x^6 - 2x^5 - 8$ .

## 6 Conclusion

In this paper, we study when a  $\sigma$ -ideal has a finite  $\sigma$ -Göbner basis. We focused on a special class of  $\sigma$ -ideals: normal binomial  $\sigma$ -ideals which can be described by the Gröbner basis of a  $\mathbb{Z}[x]$ -module. We give a criterion for a univariate normal binomial  $\sigma$ -ideal to have a finite  $\sigma$ -Gröbner basis. When the characteristic set of the  $\sigma$ -ideal consists of one  $\sigma$ -polynomial, we can give constructive criteria for the  $\sigma$ -ideal to have a finite  $\sigma$ -Gröbner basis and an algorithm to compute the finite  $\sigma$ -Gröbner basis under these criteria. One case is still not solved and we summary it as a conjecture. Also, it is desirable to extend the criteria given in this paper to multivariate binomial  $\sigma$ -ideals. Example 2.9 shows that extending Theorem 3.1 to the multivariate case is quite nontrivial. For  $\sigma$ -Gröbner basis of general  $\sigma$ -ideals, the work on monomial  $\sigma$ -ideals may be helpful [20].

## References

- [1] G.E. Collins and A.G. Akritas. Polynomial Real Root Isolation Using Descarte's Rule of Signs, *Proc. 1976 ACM Symposium on Symbolic and Algebraic Computation*, 272-275.
- [2] R. Becker, M. Sagraloff, V. Sharma, J. Xu, C. Yap. Complexity Analysis of Root Clustering for a Complex Polynomial *Proc. ISSAC '16*, 71-78, 2016, ACM Press.
- [3] R. J. Bradford and J. H. Davenport, Effective Tests for Cyclotomic Polynomials, *ISSAC 1988*, LNCS 358, 244-251, Springer, Berlin-New York, 1989
- [4] B. Buchberger. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal, *Journal of Symbolic Computation*, 41, 475-511, 2016.
- [5] R. M. Cohn. *Difference Algebra*, Interscience Publishers, New York, 1965.
- [6] D. Eisenbud and B. Sturmfels. Binomial Ideals, *Duke Math. J.*, 84(1), 1-45, 1996.
- [7] X. S. Gao, Z. Huang, C. M. Yuan. Difference Binomial Ideals, *Journal of Symbolic Computation*, 80(3), 665-706, 2017.
- [8] X. S. Gao, Y. Luo, C. M. Yuan. A Characteristic Set Method for Ordinary Difference Polynomial Systems, *Journal of Symbolic Computation*, 44(3), 242-260, 2009.
- [9] V. P. Gerdt. Consistency Analysis of Finite Difference Approximations to PDE Systems, *Proc. of MMCP 2011*, LNCS 7175, 28-C42., Springer, Heidelberg, 2012.

- [10] V. P. Gerdt and D. Robertz. Computation of Gröbner Bases for Systems of Linear Difference Equations, *Computeralgebra-Rundbrief*, Nr. 37, GI DMV GAMM, 2005, 8-13.
- [11] V. P. Gerdt and D. Robertz. Computation of Difference Gröbner Bases, *Computer Science Journal of Moldova*, 20(2), 203-226, 2012.
- [12] K. I. Iima and Y. Yoshino. Gröbner Bases for the Polynomial Ring with Infinite Variables and Their Applications, *Communications in Algebra*, 37:10, 3424-3437, 2009.
- [13] R. J. Jing, C. M. Yuan, X. S. Gao. A Polynomial-time Algorithm to Compute Generalized Hermite Normal Form of Matrices over  $\mathbb{Z}[x]$ , *arXiv:1601.01067*, 2016.
- [14] A. Levin. *Difference Algebra*, Springer, 2008.
- [15] M. V. Kondratieva, A. B. Levin, A. V. Mikhalev, E. V. Pankratiev. *Differential and Difference Dimension Polynomials*. Kluwer Academic Publishers, 1999.
- [16] B. Martin and V. Levandovskyy. Symbolic Approach to Generation and Analysis of Finite Difference Schemes of Partial Differential Equations, *Numerical and Symbolic Scientific Computing: Progress and Prospects*, 23-156, Springer, Wien, 2012.
- [17] V. Powers and T. Wörmann, An Algorithm for Sums of Squares of Real Polynomials, *Journal of Pure and Applied Algebra*, 164, 221-229, 2001.
- [18] J. F. Ritt and J. L. Doob. Systems of Algebraic Difference Equations, *American Journal of Mathematics*, **55**, 505-514, 1933.
- [19] V. Sharma and C. K. Yap. Near Optimal Tree Size Bounds on a Simple Real Root Isolation Algorithm, *Proc. ISSAC '12*, 319-326, 2012, ACM Press.
- [20] J. Wang. Monomial Difference Ideals. *Proc. AMS*, doi.org/10.1090/proc/13369, 2016.
- [21] M. Wibmer. *Algebraic Difference Equations*, Preprint, 2013.